Zhewen Zheng
University of Washington

MATH 300, Spring 2020
Week 1 Summary

Objectives

Statements, Truth Values, and Axioms

(a) We want to build a self-consistent mathematical theory from scratch where we only have some ***axioms***.

(b) We will only use ***logic***, the ***axioms***, and statements that have already been proved. We also allow for some things in this class beyond the ***axioms*** such as the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

(c) We only allow the operations $+, \cdot$ in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Division is **NOT** allowed.

(d) We also have relations $=, >, <$ and properties these relations come with.

(e) We have quantifiers ***for all*** and ***there exists***.

(f) To find a the truth value of a statement, either find a proof to show it is TRUE, or find a counterexample to show it is FALSE.

Notations

(a) To indicate that m is an integer, we write $m \in \mathbb{Z}$ as m is an element of $\mathbb{Z}$.

(b) $\mathbb{N} = \{1, 2, 3, 4 \cdots\}$ is the natural numbers, or positive integers, included in $\mathbb{Z}$.

(c) $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$ is the integers included in $\mathbb{Q}$.

(d) $\mathbb{Q} = \{\frac{p}{q} : p, q \text{integers}, q \neq 0\}$ is the rational numbers included in $\mathbb{R}$.

(e) $\mathbb{R}$ is set of the real numbers.

Definitions

Statements, Truth Value, Finding the Truth Value

(a) Defined ***statement***, ***conditional statement***, ***proof***, ***axiom***.

(b) A ***statement*** is a sentence (written in words, mathematical symbols, or a combination of the two) that is either TRUE or FALSE with no ambiguity.

(c) A statement of the form *If...then...* is called a ***conditional statement***. We call the *if*-part ***hypothesis***, the *then*-part ***conclusion***.

(d) A ***proof*** is a piece of writing that demonstrates that a particular statement is true. A statement that we prove to be true is often called a ***proposition*** or a ***theorem***. We construct proofs using logical arguments and statements that we already know to be true. But the proofs of those statements must depend on previously-proved statements and so on. If we keep tracing the statements back far enough, we must get to a point where we use a statement that we assume to be true without proof. A statement that we assume without proof is an axiom

(e) ***Axioms*** are statements we assume to be TRUE without need of proof. They build the foundation of a mathematical theory.

EPI's, Even and Odd, Parity

(a) For EPI refer to the PDF. Both part of the EPI can be used without proofs.

(b) The negative integers are the ***additive inverse*** of their position counterparts. Cannot use $-a = -1 \cdot a$ without proofs. Treat subtraction as addition of the corresponding additive inverse.

(c) Defined ***definition***, ***even and odd***, ***parity***, ***absolute value***, ***divisibility***$(|, \nmid)$.

(d) ***Even*** is equivalent to ***divisible by 2***.

(e) Two integer either has the same or opposite parity.

Proofs

(a) The first proof showed how to justify every single manipulation. We did a table format, where justifications were given in each line. Later we will use English text that deals with mathematics to write down a proof.

(b) **NEVER** use what you are about to prove.

Zhewen Zheng
University of Washington

Lecture 5 - Logic

Objective: Define statements with logic operators and learn to build a truth table.

Definition

- Let P and Q be two statements.
  (a) Then P **AND** Q is a statement that is true only if P and Q are both true. Otherwise it is false. This can be denoted by $P \wedge Q$.
  (b) Then P **OR** Q is a statement that is true if p is true or Q is true or both are true. Otherwise it is false. This can be denoted by $P \vee Q$.

Content

Steps to follow:

- Initialize a column for each statement (e.g. $P_1, P_2, \cdots, P_n$)
- Construct intermediate columns to reach the final composite statement (e.g. P_1**OR** P_2)
- There are 2^n rows to set up where n is the number of statements we need to evaluate. These resemble all possible combinations of true/false scenarios of the P_i's.
- Evaluate the truth value of each statement in their corresponding cells.

Lecture 6 - Negations

Objective: Define negation and explore negations of AND/OR statements.

Definition

- Let P be a statement. The negation of P is written as

  It is not the case that P holds.

- The negation of P is a statement which has the opposite truth value of P.
- Can be denoted as $\neg P$ (not used in our class).
- The complement of $<$ is $\geq$; complement of $>$ is $\leq$

Content

- Negation in Natural language (such as English) might be different then the rigorous definition of Mathematical Language.
- The negation of the statement **NOT**(P **OR** Q) has the same truth value as (**NOT** P) **AND** (**NOT** Q)
- A negation table for different statements for reference.

Statement	**Negation(Statement)**
P **OR** Q	**NOT** P **AND NOT** Q
P **AND** Q	**NOT** P **OR NOT** Q
if P, then Q	P **AND NOT** Q

- Remember to try to not use symbols for better readability.

Lecture 7 - Conditional Statements and their Truth value

Objective: Learn to express conditional statements and evaluate their truth value.

Definition

- Conditional statements are of the form
  - If P then Q, P implies Q, $P \Rightarrow Q$, Q if P, P only if Q, Q when/whenever P, P is sufficient for Q.
  - Here, P is the hypothesis and Q is the conclusion. If the hypothesis does not satisfy, the entire statement remains true. Only when the hypothesis is true and the conclusions is false is the entire statement false.
  - ***If*** n ***is an integer then*** Q is equivalent to ***For all integers*** n***,*** Q ***holds***.

Content

- The negation of P implies Q is the same as P **AND NOT**Q in truth values. The latter is not a conditional statement.

Lecture 8 - Contrapositives, Inverses, Converse and Equivalences

Objective: Define Contrapositives, Inverses, Converse and Equivalences.

Definition

- Let If P then Q be a conditional statement.

	Statement
Original	If P then Q
Negation	P and **NOT** Q
Converse	If Q then P
Inverse	If **NOT** P then **NOT** Q
Contrapositive	If **NOT** Q then **NOT** P

- The statement P if and only if Q, written as P implies Q, is equivalent to (P **implies** Q) **AND** (Q **implies** P).

Content

(a) The truth values of P **implies** Q, Q **implies** P, **NOT** P **implies NOT** Q are unrelated.

(b) The statement P **implies** Q has equivalent truth value as **NOT** Q **implies NOT** P.

(c) Proving equivalences require two directional proofs: $P \Rightarrow Q$ and $Q \Rightarrow P$.

Lecture 9 - Quantifiers

Definition

- We have two types of quantifiers
  (a) ***There exists*** [math.structure] such that P holds. (P might depend on [math.structure])
  (b) ***For all*** [math.structure] it holds(it is true) that P.
- We can show that a ***For all***-statement is false by giving one specific counter-example.
- We do not use the symbol $\forall$ for ***For all***, nor do we use $\exists$ for ***There exists***.

Lecture 10 - Negations of Quantified Statements

Objective: Learn how to complete sentences and then negate quantified statements step by step.

Content

- We have a scheme of treating quantified statements.
  (a) Every ***For all*** is followed by a ***it holds that (it is true that)***.
  (b) Every ***There exists*** is followed by a ***such that***.
- To negate the statement, start from the leftmost quantifier
  (a) Replace "***There exist*** ... such that Q" by "***For all*** ... it holds that **NOT** Q."
  (b) Replace "***For all*** ... it holds that Q" by "***There exists*** ... such that **NOT** Q."
- Remember we prove that a ***for all*** statement is false by proving its negation, which is a ***there exists***, is true.

Lecture 11 - Writing Proofs/Direct Proofs

Objective: Learn how to write a formal direct proof.

Content

- Format to a Proof:
  (a) Write down the statement.

(b) State the proof with *Proof:*

(c) Write down the hypothesis: "Let's assume that...", "Suppose that..."

(d) Use logic and previously obtained results to get to the conclusion.

- Use complete sentences and use "Thus, therefore, hence, also..."
- Do not use the symbols (except the qed symbols).
- We have responsibility to make it legible and clear for the reader to follow.

(e) Arrive at conclusion.

(f) Finish a proof with a □, ■, q.e.d, 'This proves the statement'.

- Direct Proofs: Start with Hypothesis and use logic to arrive at the conclusion.
- Writing out the goal we want to show helps.
- We proved "if a, b are both even then $a \cdot b$ is even.", "if $a \mid b$ and $b \mid c$ then $a \mid c$."
- Use **we** and *us* to invite the readers to follow along.

Lecture 12 - Proof by Cases

Objective: Learn how to write proof by cases

Proof

- **Theorem**
  The product of two consecutive integer is even.

  Proof. Let $n, n+1$ be two consecutive integers. Goal: $n(n+1) = 2 \cdot l$
  In the first case we let n be even. Clue: use $n = 2k$ which is given by def. of even.
  In the second case we let n be odd. Clue: use $n = 2k+1$ which is given by def. of odd. ■

- **Theorem**
  If a or b is even, then $a \cdot b$ is even.

  Proof. Assume a, b are integers.
  WLOG assume a is even. Then there is an integer k such that $a = 2k$. Substituting this in to $a \cdot b$ we have $2k \cdot b = l$.
  Therefore $a \cdot b$ is even. ■

Content

- Still a direct proof.
- Proof by Cases is used when there are more than one cases that we have to prove directly but separately assess.
- WLOG(Without Loss Of Generality): Use WLOG when proof by cases involves only variable swapped and the proof is the same. Absolute symmetry in the statements indicates permissible use of WLOG.

Definitions

(a) If n is an integer then

$$|n| = \begin{cases} n & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -n & \text{if } n < 0 \end{cases}$$

(b) A rational number q is a number of the form $q = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$.

(c) A real number that is not a rational number is called irrational number.

Lecture 13

- **Theorem (Elementary Properties of the Absolute Value)**
  Let a be an integer.
  (a) $|a| \geq 0$
  (b) $|-a| = |a|$
  (c) $-|a| \leq a \leq |a|$
  (d) $|a \cdot b| = |a| \cdot |b|$
  (e) $|a^2| = |a|^2$
  (f) $|a| \leq |b|$ if and only if $-|b| \leq a \leq |b|$
- We prove (a) using proof by cases since the definition of absolute value is naturally case dependent.
- Remember to use the EPI to justify steps.

Lecture 14

- **Theorem (Triangular Inequality)**
  If a, b are integer then
  $$|a + b| \leq |a| + |b|$$
- We will use $|a - b| \leq |a| + |b|$ instead.
- Note: Proof of this theorem involves using using part c,a,f of the **Elementary Properties of the Absolute Value**.

Lecture 15

Indirect Proofs of *If* P *then* Q

- **Proof by Contrapositive**
  - Remember that ***If*** P ***then*** Q has the same truth table as ***If NOT*** Q ***then NOT*** P.
  - This strategy is useful when we have little hypothesis but huge desired conclusion. Proving the contrapositive reverse the imbalance to our advantage.
- **Proof by Contradiction**
  - We assume ***If*** P ***then*** Q is a false statement. Then use ***NOT(If*** P ***then*** Q***)*** and try to reach a known false statement, i.e. a contradiction.
- Often equivalences are proved by direct proof in one direction and indirect proof in the other one.

Lecture 16

- **Theorem**
  Let n be an integer. Then n^2 is even ***if and only if*** n is even.
- Proving the above theorem by an indirect way is much straightforward than directly.
- It is difficult to express n when we only know something about n^2.
- Here for the ***only if*** direction we prove its contrapositive. For the ***if*** direction we prove it directly.

Lecture 17

- **Theorem**
  No integer is both even and odd.
- We prove this theorem by contradiction. First we express the theorem to its full statement.
- ***If*** n ***is integer then*** n ***is not even and odd.***
- We can do algebra normally.

Lecture 18

- **Theorem**
  $\sqrt{2}$ is an irrational number, where $\sqrt{2} \in \mathbb{R}$ such that $(\sqrt{2})^2 = 2$.
- We prove this theorem by contradiction. Hint: there is a negation in the statement.
- We assume that $\sqrt{2}$ is expressed in a simplest form $\frac{a}{b}$ without common denominator and reach a contradiction by showing both a, b are divisible by 2.

Lecture 19

- **Theorem**
  Let a be an integer. If a^2 is odd then a is odd.
- We first prove this theorem by contrapositive.
- We then prove this theorem by contradiction. We arrive at $a^2 + a$ being both odd and even, contradicting with our previously proven theorem.
- Notice the difference. For proof by contrapositive, we start at **NOT** Q and show **NOT** P. For proof by contradiction, we use both P **AND NOT** Q to arrive at a contradiction with some known fact. We do not arrive at **NOT** P.

Lecture 20

- For statement like ***for all*** $\underline{*}$ ***it holds that*** P, we prove such a statement by fixing a specific but ***arbitrary*** chosen $*$
- We should use scratch paper to assist our construction.
- **Theorem**
  Let a, b, c be integers and suppose $c \mid a$ and $c \mid b$. For all integers n, m it holds that $c \mid am+bm$.

Lecture 21

- For statement like ***There exists*** $\underline{\textit{(unique)}\ *}$ ***such that*** P, we often prove such a statement by providing a specific example, sometimes also by construction. For proof of the uniqueness, we assume a second such structure and either
  - Proving that it is already equal to the one we find previously
  - Or, under the assumption it is different, arrive at a contradiction.

Zhewen Zheng
University of Washington

Objective

(a) This week's objective is ***Set Theory***.

(b) We will not look at those axioms. We will only make the general statement about what defines sets.

Definition

(a) A ***set*** is an unordered collection of ***elements***. A set is defined by what is ***in it***.

(b) Let A, B be sets. The ***union of*** A ***and*** B denoted by $A \cup B$, is the set of all elements x such that $x \in A$ **OR** $x \in B$.

(c) Let A, B be sets. The ***intersection of*** A ***and*** B denoted by $A \cap B$ is the set of all elements x such that $x \in A$ **AND** $x \in B$.

(d) If A, B has no common elements, A, B are ***disjoint***.

(e) Let A, B be sets. The ***set difference*** $A \setminus B$ is the set of all elements of A that are not in B.

(f) Let A, B be sets. We say A ***is a subset of*** B, denoted by $A \subseteq B$, whenever the following holds

$$\text{If } x \in A \text{ then } x \in B.$$

(g) Let A, B be sets. Then $A = B$ if $A \subseteq B$ **AND** $B \subseteq A$.

(h) A set of sets is often called a ***family***.

(i) Sometimes, the members of a family are number through indices.

- Let Λ be an index set; for instance $\Lambda = \mathbb{N}$.
- Let $A_\lambda, \lambda \in \Lambda$ be a family member.
- Then $\mathcal{F} = \{A_\lambda : \lambda \in \Lambda\}$

(j) Let A be a set. Then the ***power set*** $\mathcal{P}(A)$ is the set of all subsets of A.

Lecture 22 - Intro to Sets

- Set Theory was founded by Cantor.
- Around 1900 mathematicians realized that sets in set theory was not clear about whether a given entity was an element of the set or not.
- The classic Paradox in set theory was the Barber Paradox.
- Barber Paradox: Does a Barber, who shaves all men which does not shave themselves, shaves himself?
- The problems have been fixed by the ZFC axioms.

Lecture 23 - Sets II

- We describe set element either by ***directly listing them, providing a pattern, or using the set-builder notation***.
- set-builder example: $A = \{(x, y) : x, y \in \mathbb{R}, x = y^2\}$
- If x is an element in a set A, we write $x \in A$.
- If x is not an element in a set A, we write $x \notin A$.
- Convention: lower case letters for elements, UPPER CASE for sets.
- $A = \{\} = \emptyset$ is the set with no elements.

Lecture 24 - Union of Sets

- Proofs around union are often done by cases.
- $A \cup B = B \cup A = \{x : x \in A \text{ or } x \in B\}$; $A \cup \emptyset = A$; $A \cup \mathbb{Z} = \mathbb{Z}$ where $\mathbb{Z}$ is the universal set.

Lecture 25 - Intersection of Sets

- $A \cap B = B \cap A = \{x : x \in A \text{ and } x \in B\}$; $A \cap \emptyset = \emptyset$; $A \cap A = A$

Lecture 26 - Set Difference

- $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$
- In general $A \setminus B \neq B \setminus A$.
- For all sets A, it holds that $A \setminus A = \emptyset$ and $A \setminus \emptyset = A$

Lecture 27 - Subsets

- To show $A \subseteq B$, we start with $x \in A$ and prove that $x \in B$.
- For the statement If $A \subseteq B$ then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, we must start with an $X \in \mathcal{P}(A)$ to show $X \in \mathcal{P}(B)$ using the $A \subseteq B$ in between.
- Note the difference in proof in subsets than direct proofs.
- If we are to prove $A \subseteq B$, we want to spend a line stating:

$$\text{If } A = \emptyset \text{ then the statement is clear.}$$

- The above only holds when A is an arbitrary set.
- Convention-wise, we will use $\subseteq$ and $\subsetneq$

Lecture 28 - Proofs with Sets

- **Theorem**
  Let A, B, C, D be sets. Suppose $A \subseteq B$ and $C \subseteq D$. Then $A \cup C \subseteq B \cup D$.
- If $A \cup C = \emptyset$, then the statement is clear.
- Otherwise, let $x \in A \cup C$. Then $x \in A$ **OR** $x \in C$.
- Case $x \in A$: Then $x \in B$ by hypothesis ($A \subseteq B$), Then $x \in B$ **OR** $x \in D$, thus $x \in B \cup D$.
- Case $x \in C$: Then $x \in D$ by hypothesis ($C \subseteq D$), Thus $x \in D$ **OR** $x \in B$, thus $x \in B \cup D$.
- In either case $A \cup C \subseteq B \cup D$.

Lecture 29 - Set Equality

- To prove $A = B$ we need to provide a 2-step proof: $\subseteq$ and $\supseteq$.
- **Theorem**
  Let A, B, C, D be sets. Then $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

$\subseteq$ If $A \setminus (B \cup C) = \emptyset$, then the statement is true.
Let $x \in A \setminus (B \cup C)$. Then $x \in A$ and $x \notin (B \cup C)$.
$\vdots$
Thus $x \in (A \setminus B) \cup (A \setminus C)$.

$\supseteq$ If $(A \setminus B) \cap (A \setminus C) = \emptyset$, then the $\subseteq$-relation is true.
Let $x \in (A \setminus B) \cap (A \setminus C)$.
$\vdots$
Thus $x \in A \setminus (B \cup C)$.

- We can repeat what is already true.
- Reduce the statement down to the set containment of x (whether $x \in$ or $\notin$ some set)

Lecture 30

- Set equalities of the form $A = \emptyset$, we do not use the 2-step proof of $\subseteq$ and $\supseteq$. (Avoid the problem of having nothing to pick from)
- Use indirect proof.
- **Theorem**
  Let A be a set. Then $A \setminus A = \emptyset$.
- Proof by contradiction. (A is a set and $A \setminus A \neq \emptyset$).
- Then there exists $x \in A \setminus A$. Now $x \in A$ and $x \notin A$.
- Thus $x \in A$ and **NOT**$(x \in A)$. This is a contradiction.

Lecture 31

- Sets are bags. We look inside the bag to find what is in it. The elements can be anything.
- Some Questions:

$\emptyset \in \mathbb{D}$?	Can I pull a bag of empty set out of $\mathbb{D}$?	No.
$\emptyset \subseteq \mathbb{D}$?	Is the empty set a subset of $\mathbb{D}$?	Yes.
$\{1,3,6,10,5\} \in \mathbb{D}$?	Can I pull a bag of $\{1,3,6,10,5\}$ out of $\mathbb{D}$?	Yes.
$\{5\} \in \mathbb{D}$?	Can I pull a bag of $\{5\}$ out of $\mathbb{D}$?	No.
$5 \in \mathbb{D}$?	Can I pull a 5 out of $\mathbb{D}$?	No.
$5 \subseteq \mathbb{D}$?	Is the 5 a subset of $\mathbb{D}$?	No.

- The empty set is a subset of any set.
- An individual element of a set A is not necessarily a subset of A.

Lecture 32

- The power set of a given set A is a family.
- If a set A has n elements, then the power set of A has 2^n elements. Use this fact to check if the power set is completely constructed.
- The power set could have infinitely many elements depending on what A is.
- The power set is never the empty set because it always contains the empty set.

Lecture 33

- **Theorem**
  Let A, B be sets. Then $\mathcal{P}(A) \subseteq \mathcal{P}(A \cup B)$

Lecture 34

- **Theorem**
  Let A, B be sets. Then $A \cap B = \emptyset$ if and only if $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset\}$.
- Two part proof:
  (a) Assume $A \cap B = \emptyset$. Show $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset\}$.
  If $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\emptyset\}$ then $A \cap B \neq \emptyset$.
  Then since $\mathcal{P}(*)$ always contains $\emptyset$, there must be a set $X \in \mathcal{P}(A) \cap \mathcal{P}(\mathcal{B})$ and $X \neq \emptyset$.
  $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$. By definition of power set, $X \subseteq A$ and $X \subseteq B$.
  Thus, for any $x \in X \neq \emptyset$ it holds that $x \in A$ and $x \in B$.
  thus $A \cap B \neq \emptyset$.
  (b) Assume $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset\}$. Show $A \cap B = \emptyset$.
  If $A \cap B \neq \emptyset$ then $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\emptyset\}$.
  Then there exists $x \in A \cap B$. So, $x \in A$ and $x \in B$. Then $\{x\} \subseteq A$ and $\{x\} \subseteq B$. By definition of power set, $\{x\} \in \mathcal{P}(A)$ and $\{x\} \in \mathcal{P}(B)$.
  Thus $\{x\} \in \mathcal{P}(A) \cap \mathcal{B}$ which implies $(A \cap B) \neq \{\emptyset\}$.

Lecture 35

Objective: Define Family Union.

Definition

- Let $\mathcal{A} = \{A_\lambda : \lambda \in \Lambda\}$ be a family. Then the ***family union***

$$\begin{aligned}\bigcup \mathcal{A} &= \{a : \text{there is } \lambda \in \Lambda \text{ such that } a \in A_\lambda\} \\ &= \{a : \text{there is } A \in \mathcal{A} \text{ such that } a \in A\}\end{aligned}$$

- Any element in $\bigcup \mathcal{A}$ will come from some element in some of the sets of $\mathcal{A}$.

Content

- $\mathcal{A} = \{A_\lambda : \lambda \in \Lambda\}$

$$\begin{aligned}\mathcal{A} &= \{A_i : i \in \mathbb{N}, A_i = [-i, i]\} \\ &= \{A_i = [-1, 1], A_2 = [-2, 2], A_3 = [-3, 3], \cdots\}\end{aligned}$$

- Think of ***family union*** as opening up all the inner sets to extract the contents.
- Remember the difference. $\bigcup \mathcal{A}$ is generally a set; it could be a family. $\mathcal{A} \cup \mathcal{B}$ remains as a family.

Lecture 36

Objective: Define Family Intersection.

Definition

- Let $\mathcal{A} = \{A_\lambda : \lambda \in \Lambda\}$ be a family. Then the ***family intersection***

$$\begin{aligned}\bigcap \mathcal{A} &= \{a : a \in A_\lambda \text{ for all } \lambda \in \Lambda\} \\ &= \{a : a \in A \text{ for all } A \in \mathcal{A}\}\end{aligned}$$

Content

- Think of ***family intersection*** as finding contents in the inner sets that occurs in all inner sets.
- Note that proofs with $\cup, \cap$ should strictly work with the definition.

Lecture 37

Objective: Proofs around Family Intersection/Union I

Proof

- **Theorem**
  Let $\mathcal{F}, \mathcal{G}$ be families. Then

$$\bigcup(\mathcal{F} \cup \mathcal{G}) = (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$$

- For this kind of equality, we have to show $\subseteq$ and $\supseteq$

$\subseteq$ If $\bigcup(\mathcal{F} \cup \mathcal{G}) = \emptyset$, the statement is clear.
Else, let $x \in \bigcup(\mathcal{F} \cup \mathcal{G})$. We need to show $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$
Then there is $A \in \mathcal{F} \cup \mathcal{G}$.
Without the loss of generality $A \in \mathcal{F}$. Thus $x \in A \in \mathcal{F}$. We need to show $x \in A \in \mathcal{F}$ **OR** $x \in B \in \mathcal{G}$
which implies $x \in \bigcup \mathcal{F}$
Then it is true that $x \in \bigcup \mathcal{F}$ **OR** $x \in \bigcup \mathcal{G}$, thus $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.

$\supseteq$ If $(\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G}) = \emptyset$, the statement holds.
Let now $x \in (\bigcup \mathcal{F} \cup \bigcup \mathcal{G})$.
WLOG $x \in \bigcup \mathcal{F}$. Then there is $A \in \mathcal{F}$ and $x \in A$.
This means $x \in A$ and $A \in \mathcal{F} \cup \mathcal{G}$, which $\bigcup(\mathcal{F} \cup \mathcal{G})$.

Lecture 38

Objective: Proofs around Family Intersection/Union II

Proof

- **Theorem**
  Suppose $\mathcal{F}, \mathcal{G}$ are families with $\mathcal{F} \neq \emptyset$ and $\mathcal{G} \neq \emptyset$. Then it holds that If $\mathcal{F} \subseteq \mathcal{G}$ than $\bigcap \mathcal{G} \subseteq \bigcap \mathcal{F}$.
- If $\bigcap \mathcal{G} = \emptyset$, the statement is clear.
  Let $x \in \bigcap \mathcal{G}$. Thus $x \in A4$ for all $A \in \mathcal{G}$.
  Let $\underbrace{A}_{\text{arbitrary and exists}} \in \mathcal{F}$. Thus $A \in \mathcal{G}$, thus $x \in A$.
  This means $x \in A$ for all $A \in \mathcal{F}$.

Lecture 39

Objective: Proofs around Family Intersection/Union III

Proposition

- Consider $\mathcal{A} = \{A_i : A_i = [\frac{1}{i}, 1], i \in \mathbb{N}\}$.
  Then $\bigcup \mathcal{A} = \bigcap_{i \in \mathbb{N}} A_i = (0, 1]$

Explore

- We need to explore the family in detail.

$$A_1 = [1,1] = \{x : 1 \leq x \leq 1\}$$
$$A_2 = \left[\tfrac{1}{2},1\right] = \{x : \tfrac{1}{2} \leq x \leq 1\}$$
$$A_3 = \left[\tfrac{1}{3},1\right] = \{x : \tfrac{1}{3} \leq x \leq 1\}$$
$$A_4 = \left[\tfrac{1}{4},1\right] = \{x : \tfrac{1}{4} \leq x \leq 1\}$$

Proof

$\subseteq$ Let $x \in \bigcap \mathcal{A}$. Thus there is A_i such that $x \in A_i$ for some $i \in \mathbb{N}$.
So $x \in [\frac{1}{i}, 1]$ i.e. $\frac{1}{i} \leq x \leq 1$.
As $i \in \mathbb{N}$, we have $0 < \frac{1}{i}$, so $0 < \frac{1}{i} \leq x \leq 1$, in particular $x \in (0,1]$

$\supseteq$ Let $x \in (0,1]$, i.e. $0 < x \leq 1$
(Archimedean Property) $\mathbb{N}$ is unbounded.
So there will be $i \in \mathbb{N}$ such that $i > \frac{1}{x}$.
But this implies $\frac{1}{i} < x$, so $x \in [\frac{1}{i}, 1] = A_i$
Thus, $x \in A_i$ and therefore $x \in \bigcup\limits_{i \in \mathbb{N}} = \bigcup \mathcal{A}$

Lecture 40

Objective: Find a new way to prove statements involving the natural numbers.

Content

- Prove the statement for the smallest value of $n \in \mathbb{N}$. (Base Case)
- Set up the Induction Hypothesis (IH): Assume $P(k)$ is true.
- Prove that if the statement is true for some $k \in \mathbb{N}$, then it is true for $k+1$. (Induction Step).
- Understand Mathematical Induction as ***setting up a sequence of dominos so that when the first case falls, everything that follows consequently falls***.
- We need to clearly mark when the IH is used.
- We need to have the goal $P(k+1)$ in mind.
- By the PMI the statement $P(n)$ is true for all $n \geq$ base case.

Lecture 41

Objective: Examples for Induction

Definition

- $m \in \mathbb{Z}, n \in \mathbb{N}$, then $m^n = \underbrace{m \cdot m \cdot m \cdots m}_{n\text{times}}$

Proof

- **Theorem**
  For every $n \in \mathbb{N}, 3 \mid 7^n - 1$.

- Proof: By Induction.
- Base case: $n-1$. Then

$$7-1=6, 3 \mid 6$$

- IH: Assume $3 \mid 7^n - 1$
- Induction Step: (Prove $3 \mid 7^{k+1}-1$ using IH)

  We know that $3 \cdot l = 7^k - 1$ for some $l \in \mathbb{N}$ by IH, so $7^k = 3l+1$.
  Then

$$7^{k+1} - 1 = 7 \cdot 7^k - 1 \underbrace{=}_{IH} 7(3l+1) - 1 = 21l + 7 - 1 = 21l + 6 = 3(7l+2)$$

  Proving that $3 \mid 7^{k+1} - 1$
- By the PMI the statement is therefore true.

Lecture 42

Objective: Examples for Induction

Proof

- **Theorem**
  For every $n \in \mathbb{N}, 5 \mid 8^n - 3^n$
- Proof: By Induction.
- Base Case: $n = 1, 8^1 - 3^1 = 5$ and $5 \mid 5$.
- IH: Assume $5 \mid 8^k - 3^k$ for <u>some</u> $k \in \mathbb{N}$.
- Induction Step:

  As $5 \mid 8^k - 3^k$, there exists $l \in \mathbb{Z}$ such that $5 \cdot l = 8^k - 3^k \Leftrightarrow 3^k = 8^k - 5l$

$$\begin{aligned} 8^{k+1} - 3^{k+1} &\underbrace{=}_{IH} 8^{k+1} - 3 \cdot (8^k - 5l)) = 8^{k+1} - 3 \cdot 8^k + 15l \\ &= 8^k(8-3) + 15l = 8^k \cdot 5 + 15l = 5(8^k + 3l) \end{aligned}$$

  Proving that $5 \mid 8^{k+1} - 3^{k+1}$
- By the PMI the statement is true for all $n \in \mathbb{N}$

Lecture 43

Objective: Sums and Induction

Definition

- $a_1 + a_2 + a_3 + \cdots + a_n = \sum_{i=1}^{n} a_i$
- $a_1 + a_2 + a_3 + \cdots + a_n + a_{n+1} = \sum_{i=1}^{n+1} a_i = (\sum_{i=1}^{n} a_i) + a_{n+1}$
- $a_1 + a_2 + a_3 + \cdots + a_n = \sum_{i=1}^{n} a_i \underbrace{=}_{i+1=j, j=i-1} \sum_{j=2}^{n+1} a_{j-1}$
- $a_1 + a_2 + a_3 + \cdots + a_n = \sum_{i=1}^{n} a_i = a_n + a_{n-1} + \cdots + a_2 + a_1 = \sum_{j=1}^{n} a_{n+1-j}$

Lecture 44

Proof

- **Theorem**
  For every $n \in \mathbb{N}, \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.
- Proof: By Induction.
- Base Case: $n = 1$. Then $\sum_{i=1}^{1} i = 1 = \frac{1+1}{2}$
- IH: Assume $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ for some $k \in \mathbb{N}$.
- Induction Step:

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + k + 1 \\ &= \frac{k(k+1)}{2} + k + 1 = \frac{k(k+1) + 2k + 2}{2} \\ &= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}\end{aligned}$$

  By the PMI, $\sum_{i=1}^{n} = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

Lecture 45

Objective: Define Products and Factorial

Definition

- Let $n \in \mathbb{N}, a_i \in \mathbb{R}$ where $1 \leq i \leq n$.

$$a_1 \cdot a_2 \cdot a_3 \cdots a_n = \prod_{i=1}^{n} a_i$$

$$\prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^{n} a_i\right) \cdot a_{n+1}$$

- $$\prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot 4 \cdots n = n!$$

- $0! = 1$.

Lecture 46

Objective: Proof by Induction on Products

Proof

- **Theorem**
  For all $n \in \mathbb{N}, \prod_{i=1}^{n}(4i - 2) = \frac{(2n)!}{n!}$.

- Base case: $n = 1$

$$\prod_{i=1}^{1}(4i-2) = (4 \cdot 1 - 2) = 2$$

$$\frac{(2 \cdot 1)!}{1!} = \frac{2}{1} = 2$$

- IH: Assume $\prod_{i=1}^{k}(4i-2) = \frac{(2k)!}{k!}$ for <u>some</u> $k \in \mathbb{N}$.
- Induction Step: Then

$$\begin{aligned}\prod_{i=1}^{k+1}(4i-2) &= \left(\prod_{i=1}^{k}(4i-2)\right) \cdot (4(k+1)-2) = \frac{(2k)!}{k!}(4k+4-2) \\ &= \frac{(2k)!}{k!} \cdot (4k+2) = \frac{(2k)!}{k!} \cdot \underbrace{\frac{k+1}{k+1}}_{\text{smart 1}} \cdot (4k+2) \\ &= \frac{(2k)!}{(k+1)!}\frac{(k+1)2(2k+1)}{1} = \frac{(2k)!(2k+1)(2k+2)}{(k+1)!} = \frac{(2(k+1))!}{(k+1)!}\end{aligned}$$

  By the PMI the statement is true for all $n \in \mathbb{N}$.

■

- **Note:** Do not hesitate to force the term to be what you aim were aiming for. (such as using the smart 1).

Lecture 47

Objective: Inequalities and Induction

Content

- We need to be bold. Get rid of terms you do not need and add ones you need.
- In the Induction Step, consider where to start
  - which side leads you to IH fast and easy.
  - In inequalities, it is easier to get rid of terms than creating some.

Proof

- **Theorem**
  For all $n \in \mathbb{N}, 2^n \geq 2n$.
- Proof: By induction.
- Base case: $n = 1$: $2^1 = 2 = 2 \cdot 1$.
- IH: Assume that $2^k \geq 2k$ for <u>some</u> $k \in \mathbb{N}$.
- Induction Step:

$$2^{k+1} = 2 \cdot 2^k \underbrace{\geq}_{IH} 2 \cdot (2k) = 2k + 2k \underbrace{\geq}_{k \in \mathbb{N}, k \geq 1} 2k + 2 \cdot 1 = 2k + 2 = 2(k+1)$$

  By the PMI $2^n \geq 2n$ for all $n \in \mathbb{N}$.

■

Lecture 48

Objective: Inequalities and Induction

Proof

- **Theorem**
  For all $n \in \mathbb{N}, n! \leq n^n$.
- Proof: By Induction.
- Base Case: $n = 1$: $1! = 1 \leq 1$.
- IH: Assume $k! \leq k^k$ for some $k \in \mathbb{N}$.
- Induction Step:

$$\begin{aligned}(k+1)! = (k+1) \cdot k! &\underbrace{\leq}_{IH} (k+1) \cdot k^k = (k+1) \underbrace{k \cdot k \cdot k \cdots k}_{k} \\ &\underbrace{\leq}_{k<k+1} (k+1) \cdot \underbrace{(k+1) \cdot (k+1) \cdots (k+1)}_{k \text{ times}} \\ &= (k+1)^{k+1}\end{aligned}$$

  By the PMI $n! \leq n^n$ for all $n \in \mathbb{N}$.

■

Lecture 49

Objective: Resolve Problem on Inequalities and Induction

Problem

- Find the smallest natural number N such that $2^n > n^2$ for all $n \geq N$. Prove that you are right.

Explore

n	1	2	3	4	5	6	7
2^n	2	4	8	16	32	64	128
n^2	1	4	9	16	25	36	49

Proof

- Claim: $N = 5$ is the smallest natural number such that $2^n > n^2$ for all $n \geq N = 5$.
- Proof: By induction.
- Base Case: $n = 5$: $2^5 = 32 > 25 = 5^2$
- IH: Assume $2^k > k^2$ for some $k \geq 5$.

- Induction Step: Goal:$2^{k+1} > (k+1)^2 = k^2 + 2k + 1$

$$\begin{aligned}
2^{k+1} = 2 \cdot 2^k &\underbrace{>}_{IH} 2 \cdot k^2 \\
&\geq k^2 + k \cdot k = k^2 + \underbrace{k + k + \cdots + k}_{k \text{ times}, k \geq 5} \\
&\underbrace{>}_{k \geq 5} k^2 + k + k + k \\
&\underbrace{>}_{k \geq 5} k^2 + k + k + 1 \\
&= k^2 + 2k + 1 = (k+1)^2
\end{aligned}$$

By the PMI $2^n > n^2$ for all $n \geq 5$. Further, we note that $2^4 = 16 = 4^2$, so the inequality does not hold for $n < 5$. ■

Second Principle of Mathematical Induction

- The logic of this proof is not so different than the regular Principle of Mathematical Induction. The only difference is that for the Second Principle of Mathematical Induction, The Induction Hypothesis Assumes

  $$\text{For } \textbf{\textit{every}}\ k \in \mathbb{Z} \text{ with } k \geq M, \text{ if } \{M, M+1, \cdots, k\} \subseteq T, \text{ then } (k+1) \in T.$$

  The Base Cases are the same. However, the Induction Hypothesis and Inductive Step has a slight variation. In a sense this new kind of induction has a stronger assumption, as the Inductive Step needs all previous statements are true and uses ***this*** assumption to prove the next statement is true. The proof still work because the process is still inductive, though it happens to use more than one previous cases of k that has been proven to be true to finish the proof on $k+1$.

Problem Type: Summation/Product/Division:

(h) Prove by induction that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

Solution:

Theorem
For every $n \in \mathbb{N}, \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

Proof. By Induction.

- Base Case: $n = 1$. Then $\sum_{i=1}^{1} i^2 = 1 = \frac{1 \cdot 2 \cdot 3}{6} = \frac{1(1+1)(2 \cdot 1+1)}{6}$
- IH: Assume $\sum_{i=1}^{k} i^2 = \frac{k(k+1)(k+2)}{6}$ for some $k \in \mathbb{N}$
- Induction Step: WTS: $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \left(\sum_{i=1}^{k}\right) + (k+1)^2 \\
&\underbrace{=}_{IH} \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)(k+1)}{6} \\
&= \frac{(k+1)(k(2k+1)+6(k+1))}{6} \\
&= \frac{(k+1)(2k^2+k+6k+6)}{6} \\
&= \frac{(k+1)(2k^2+7k+6)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}
\end{aligned}$$

■

Problem Inequalities:

(c) Find the smallest $k \in \mathbb{N}$ such that $n! > n^4$ for all $n \geq k$ and prove your claim.

Solution:

Claim: $n = 7$ is the smallest $k \in \mathbb{N}$ such that $n! > n^4$ for all $n \geq k$.

Proof. By Induction.

- Base Case: $n = 7, 7! = 5040 > 2401 = 7^4$
- IH: Assume $k! > k^4$ for some $k \geq 7$.
- Induction Step: Goal: $((k+1)! > (k+1)^4 = k^4 + 4k^3 + 6k^2 + 4k + 1$

$$\begin{aligned}
(k+1)! = k!(k+1) &\underbrace{>}_{IH} k^4(k+1) = k^5 + k^4 = k^1k^4 + k^4 \\
&> \underbrace{k^4 + k^4 + \cdots + k^4}_{k \text{ times}} + k^4 \\
&\underbrace{>}_{k \geq 7} k^4 + k^4 + k^4 + k^4 + k^4 \\
&\underbrace{>}_{k \geq 7} k^4 + 4k^3 + k^4 + k^4 + k^4 \\
&\underbrace{>}_{k \geq 7} k^4 + 4k^3 + 6k^2 + k^4 + k^4 \\
&\underbrace{>}_{k \geq 7} k^4 + 4k^3 + 6k^2 + 4k + k^4 \\
&\underbrace{>}_{k \geq 7} k^4 + 4k^3 + 6k^2 + 4k + 1 \\
&= (k+1)^4
\end{aligned}$$

- By the PMI $n! > n^4$ for all $n \geq 7$.
- Further, we note that $6! = 720 < 1296 = 6^4$, so the inequality does not hold for $n < 7$. ∎

Problem Other:

(a) Prove by induction that for all real numbers a and all natural numbers n it is true that

$$(a+1)^n = \sum_{k=0}^{n} \binom{n}{k} a^k.$$

Here, we define for $n \geq k > 0$, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ and $\binom{n}{0} = 1$. Note that $\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$. First prove that

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}. \tag{1}$$

and use it later in the induction.

Solution:

Proof. First we prove that

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-(k+1))!} \\
&= \frac{n!(k+1)!(n-k-1)!}{k!(n-k)!(k+1)!(n-k-1)!} + \frac{n!k!(n-k)!}{k!(n-k)!(k+1)!(n-k-1)!} \\
&= \frac{n!(k+1)!(n-k-1)! + n!k!(n-k)!}{k!(n-k)!(k+1)!(n-k-1)!} \\
&= \frac{n!k!(k+1)(n-k-1)! + n!k!(n-k-1)!(n-k))}{k!(n-k)!(k+1)!(n-k-1)!} \\
&= \frac{n!k!(n-k-1)!((k+1)+(n-k)}{k!(n-k)!(k+1)!(n-k-1)!} \\
&= \frac{n!(n+1)}{(k+1)!(n-k)!} \\
&= \frac{(n+1)!}{(k+1)!((n+1)-(k+1))!} \\
&= \binom{n+1}{k+1}
\end{aligned}$$

Then we use proof by induction. We can actually prove the binomial theorem

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

and substituting $b = 1$ as a particular case of the theorem.

- Base Case: $n = 1$. Then $(a+b)^1 = a + b = b^1 + a^1 = \sum_{k=0}^{1} \binom{1}{k} a^k b^{n-k}$.
- IH: Assume $(a+b)^l = \sum_{k=0}^{l} \binom{l}{k} a^k b^{l-k}$ for some $l \in \mathbb{N}$.

- Induction Step:

$$\begin{aligned}
(a+b)^{l+1} &= (a+b)^l(a+1) \\
&\underbrace{=}_{IH}(a+b)\cdot\sum_{k=0}^{l}\binom{l}{k}a^k b^{n-k} \\
&= \sum_{k=0}^{l}\binom{l}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{l}\binom{l}{k}a^k b^{n-k+1} \\
&= \sum_{k=1}^{l+1}\binom{l}{k-1}a^k b^{l-k+1} + \left(\sum_{k=1}^{l}a^k b^{l-k+1} + b^{l-0+1}\right) \\
&= a^{l+1}\cdot b^0 + \left(\sum_{k=1}^{l}\binom{l}{k-1}a^k + \sum_{k=1}^{l}a^k b^{l-k+1}\right) + b^{l+1} \\
&= a^{l+1} + b^{l+1} + \sum_{k=1}^{l}\left(\binom{l}{k-1} + \binom{l}{k}\right)a^k b^{l-k+1} \\
&\underbrace{=}_{(1)}\binom{l+1}{l+1}a^{l+1}b^0 + \binom{l+1}{0}a^0 b^{l+1} + \sum_{k=1}^{l}\binom{l+1}{k}a^k b^{l-k+1} \\
&= \sum_{k=0}^{l+1}\binom{l+1}{k}a^k b^{l-k+1}
\end{aligned}$$

- By the PMI the binomial theorem is true.
- Substituting $b = 1$ we have

$$\begin{aligned}
(a+1)^n &= \sum_{k=0}^{n}\binom{n}{k}a^k\cdot 1^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^k
\end{aligned}$$

■

Zhewen Zheng
University of Washington

Lecture 50 - Division Theorem

Objective: To see a complex proof including many tools that we know

Proof

- **Theorem**
  For every pair of natural numbers m, n there exists unique nonnegative integers q and r with $0 \leq r < m$ such that
  $$n = q \cdot m + r$$
- *Proof.* – This is a existence and uniqueness theorem. We will prove existence first.
  - Case 1: $m = 1$, then for any $n \in \mathbb{N}$ it holds that
    $$n = \underbrace{n}_{q} \cdot \underbrace{1}_{m} + \underbrace{0}_{r}, 0 \leq r < 1$$
  - Case 2: $m > 1$. We need to show that for every integer $n > 0$ there exist nonnegative integers q and r such that $n = q \cdot m + r, 0 \leq r < m$.
    By Induction over n.
    Base Case: $n = 1$ Then
    $$1 = \underbrace{0}_{q} \cdot m + \underbrace{1}_{r}, 0 \leq r = 1 < m$$
    IH: Assume k is a positive integer such that
    $$k = q \cdot m + r, 0 \leq r < m$$
    Induction Step: $k + 1 = \tilde{q}m + \tilde{r}$
    By IH, $k + 1 = q \cdot m + r + 1$
    $$0 \leq r < n0 \leq r + 1 \leq m$$
    If $r + 1 < m$, we are done:
    $$k + 1 = q \cdot m + \underbrace{(r + 1)}_{\tilde{r}}, \tilde{r} < m$$
    If $r + 1 = m$, then
    $$k + 1 = q \cdot m + m = \underbrace{(q + 1)}_{\tilde{r}} \cdot m + \underbrace{0}_{\tilde{r}}$$
    Thus $k + 1 = \tilde{q} \cdot m + \tilde{r}$, where $\tilde{r} = 0$, so $0 \leq \tilde{r} < m$.
    By the PMI the statement holds.
  - We now prove the uniqueness part.

– for q, r if m, n are given.
Assume that

$$n = q_1 m + r_1 = q_2 m + r_2, 0 \leq r_1 < m, 0 \leq r_2 < m \tag{2}$$

WLOG $r_2 \geq r_1$
Then (2) can be rearranged:

$$(q_1 - q_2) \cdot m = r_2 - r_1 \tag{3}$$

This implies $m \mid r_2 - r_1$

$$r_1 \leq r_2, r_2 - r_1 \geq 0$$
$$r_2 < m, 0 \leq r_2 - r_1 < r_2 < m$$

Therefore we have $m \mid r_2 - r_2$ and $- \leq r_2 - r_1 < m$.
Then $r_2 - r_1 = 0$, i.e. $r_2 = r_1$.
By (3) we get now $(q_1 - q_2) \cdot m = 0$, so $q_1 = q_2$. ∎

Lecture 51 - Cartesian Products

Objective: Define Cartesian Product

Content

- We are moving away from proof methods to mathematical content.
- Starting with relations, eventually we will study functions, and understand its properties.

Definition

- Let A, B be sets. We define the Cartesian Product of A and B as the set of all ordered pairs $9a, b)$, where $a \in A$ and $b \in B$.
- We denotes this set by $A \times B$,

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

- We say $(a_1, b_1) = (a_2, b_2)$ if $a_1 = a_2$ and $b_1 = b_2$, where $a_1, a_2 \in A, b_1, b_2 \in B$.

Example

- $A = \{1, 2, 3\}, B = \{f, g\}, A \times B = \{(1, f), (1, g), (2, f), (2, g), (3, f), (3, g)\}$
- $A = B = \mathbb{Z}$ Then $A \times B = \{(a, b) : a \in \mathbb{Z}, b \in \mathbb{Z}\}$. ($\rightarrow$ Lattice in $\mathbb{R} \times \mathbb{R}$)
- $A = \emptyset, B$ is a set, $A \times B = \emptyset$.
- In general, $A \times B \neq B \times A$. The order matters.

Lecture 52 - Cartesian Product Problems

Proof

- **Theorem**
  Let A, B, C be sets such that $A \subseteq B$. Then $A \times C \subseteq B \times C$.
- *Proof.* If $A \times C = \emptyset$, the statement is clear.
  Otherwise we let $(a, c) \in A \times C$. Then $a \in A$ and $c \in C$.
  By hypothesis, $a \in B$, so $(a, c) \in B \times C$. ∎
- **Theorem**
  let A, B, C, D be sets. Then
  $$(A \cap B) \times (C \cap D) \subseteq (A \times C) \cap (B \times D)$$
- *Proof.* If $(A \cap B) \times (C \cap D) = \emptyset$, the statement is clear.
  Otherwise we let $(x, y) \in (A \cap B) \times (C \cap D)$.
  Then $x \in A \cap B$ and $y \in C \cap D$.
  So $x \in A$ and $x \in B$ and $y \in C$ and $y \in D$
  So $x \in A$ and $y \in C$ and $x \in B$ and $y \in D$,
  So $(x, y) \in A \times C$ and $(x, y) \in B \times D$
  Thus $(x, y) \in (A \times C) \cap (B \times D)$. ∎
- $B \times B = B^2$, $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$
- We can extend to any ordered list $A_1 \times A_2 \times \cdots \times A_n$.

Lecture 53 - Relations

Objective: Introduction to Relations

Definition

- Let A, B be sets. A <u>relation from A to B</u> is a subset of $A \times B$.
- If $A = A$ and $\mathcal{R}$ is a relation from A to A, we often say that <u>$\mathcal{R}$ is a relation on A</u>.

Example

-

Weight	Price
20g	\$0.5
30g	\$0.5
100g	\$1.00
200g	\$1.25
500g	\$2.15

  $\mathcal{R} = \{(20, 0.5), (30, 0.5), (100, 1.00), (200, 1.25), (500, 2.15)\} \subseteq A \times B$.
- $A = B = \{1, 2, 3, 4, 5, 6\}$

$$\begin{aligned}\mathcal{R} = \{(a, b) : a, b \in A, a \mid b\} = &\{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6),\\ &(2,2), (2,4), (2,6),\\ &(3,3), (3,6),\\ &(4,4), (5,5), (6,6)\}\end{aligned}$$

- $\mathcal{R} = \{(1, 11), (1, -7), (2, 3), (-5, 99), (100, 100)\} \subseteq \mathbb{Z} \times \mathbb{Z}$.

Content

- A Relation does not have to come with a particular rule of expression.
- A Relation holds when we have a ***set of ordered pairs*** where all first entries from one set and all second entries from the other.
- Keep the structure of relation in mind.

Lecture 54

Objective: Relations with specific properties: reflexive, symmetric, transitive

Definition

- Let A be a set, let $\mathcal{R}$ be a relation on A.

  (a) We say $\mathcal{R}$ is reflexive if

  $$\text{For all } a \in A\text{: } (a, a) \in \mathcal{R}$$

  (b) We say $\mathcal{R}$ is symmetric if

  $$\text{If } (a, b) \in \mathcal{R} \text{ then } (b, a) \in \mathcal{R}$$

  (c) We say $\mathcal{R}$ is transitive if

  $$\text{If } (a, b) \in \mathcal{R} \text{ and } (b, c) \in \mathcal{R} \text{ then } (a, c) \in \mathcal{R}$$

Content

- $A = \{1, 2, 3, 4, 5, 6\}, \mathcal{R} = \{(a, b) \in A \times A : a \mid b\}$
  $\mathcal{R}$ is reflexive
  $\mathcal{R}$ is not symmetric
  $\mathcal{R}$ is transitive.
- $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : (x - \frac{1}{2})^2 + (y - \frac{1}{2})^2 > \frac{1}{25}\}$
  $\mathcal{R}$ is not reflexive: $(\frac{1}{2}, \frac{1}{2})$.
  $\mathcal{R}$ is symmetric: By commutativity.
  $\mathcal{R}$ is not transitive: $(\frac{1}{2}, 0) \in \mathcal{R}, (0, \frac{1}{2} \in \mathcal{R}), (\frac{1}{2}, \frac{1}{2} \notin \mathcal{R})$

Lecture 55

Definition

- Notation: Let A, B be sets, let $\mathcal{R}$ be a relation from A to B. If $(a, b) \in \mathcal{R}$, we also write

  $$a \sim b, a\mathcal{R}b, (a, b) \in \mathcal{R}$$

- Let $\mathcal{R}$ be a relation on a set $A(\mathcal{R} \subseteq A \times A)$. Then $\mathcal{R}$ is an equivalence relation if $\mathcal{R}$ is reflexive, symmetric and transitive.
- Note: If $\mathcal{R}$ is not an equivalence relation it suffices to show that one of reflexively, symmetry, transitivity is not given.

Lecture 56

Example

- Consider the relation $\mathcal{R}$ on $\mathbb{Z} \times \mathbb{Z}$ given by

$$\underbrace{(a,b) \sim (c,d)}_{((a,b),(c,d) \in \mathcal{R})} \text{ if and only if } a+d = b+c$$

  then $\mathcal{R}$ is an equivalence relation.
- *Proof.* We prove reflexivity, symmetry, and transitivity. (by the scheme)
  - (R) SCHEME: for all $a \in A : a \sim a$
    Let $(x,y) \in A$. Then $x+y = y+x$, so $(x,y) \sim (x,y)$
  - (S) SCHEME: if $(a,b) \in \mathcal{R}$ then $(b,a) \in \mathcal{R}$
    Let $((x,y),(m,n)) \in \mathcal{R}$, so $x+y = y+m$.
    Thus $y+m = x+n$ and therefore $m+y = n+x$, which gives $((m,n),(x,y)) \in \mathcal{R}$.
  - (T) SCHEME: if $a \sim b, b \sim c$ then $a \sim c$.
    Let $(m,n) \sim (p,q), (p,q) \sim (x,y)$. Then $m+q = n+p, p+y = q+x$.
    Then $m = n+p-q, y = q+x-p$, which gives $m+y = n+p-q+q+x-p = n+x$.
    Thus $(m,n) \sim (x,y)$. ∎

content

- Remember that ***if*** $\mathcal{R} \subseteq A \times A$***, then*** $\mathcal{R}$ ***is a relation on*** A. Hence if $\mathcal{R} \subseteq (\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z})$ then $\mathcal{R}$ is a relation on $\mathbb{Z} \times \mathbb{Z}$.
- Use the structure of relation to decompose the nested complex structures such as $\mathbb{Z} \times \mathbb{Z}$.

Lecture 57 - Example Equivalence Relations

Example

- Let $\mathcal{R}$ be the relation on A, which is the set of all real functions with domain $\mathbb{R}$, defined as

$$f \sim g \text{ if there is } c \in \mathbb{R} \setminus \{0\} \text{ such that } f(x) = c \cdot g(x) \text{ for all } x \in \mathbb{R}.$$

  Show $\mathcal{R}$ is an equivalence relation.
- *Proof.* We prove reflexivity, symmetry, and transitivity one by one.
  - (R) Let $f \in A$.
    Then $f(x) = 1 \cdot f(x)$ for all $x \in \mathbb{R}$.$(c = 1+0)$ so $f \sim f$.
  - (S) Let $f \sim g$. Then there is $c \neq 0$ such that $f(x) = c \cdot g(x)$ for all $x \in \mathbb{R}$.
    Thus $g(x) = \underbrace{\frac{1}{c}}_{c \neq 0}$, so as $\underbrace{\frac{1}{c}}_{\neq 0} \subseteq \mathbb{R}, g \sim f$.
  - (T) Let $f \sim g, g \sim h$. Then there are $c_1, c_2 \neq 0$ such that $f(x) = c_1 g(x)$ and $g(x) = c_2 h(x)$ for all $x \in \mathbb{R}$.
    Thus $f(x) = \underbrace{c_1 \cdot c_2}_{\neq 0} h(x) = \tilde{c} h(x)$ thus $f \sim h$. ∎

Lecture 58 - Example Equivalence Relations

Example

- Let $A = \{a, b, c\}$. Find all equivalence relations on A.
  $\mathcal{R}_1 = \{(a,a), (b,b), (c,c)\}$
  $\mathcal{R}_2 = \{(a,a), (b,b), (c,C), (a,b), (b,a)\}$
  $\mathcal{R}_3 = \{(a,a), (b,b), (c,c), (a,c), (c,a)\}$
  $\mathcal{R}_3 = \{(a,a), (b,b), (c,c), (b,c), (c,b)\}$
  $\mathcal{R}_4 = \{(a,a), (b,b), (c,c), (a,b), (b,a), (a,c), (c,a), (b,c), (c,b)\} = A \times A$
- On the set A there are exactly 5 equivalence relations.

Lecture 59 - Equivalence Classes

Objective: Define Equivalence Classes

Definition

- Let A be a set and $\mathcal{R}$ be an equivalence relation on A.
  Then for $a \in A$, we define

$$[a] = \bar{a} = [a]_{\mathcal{R}} = \{b \in A : \text{ such that } (a,b) \in \mathcal{R}\} \subseteq A$$

Content

- With a set, on which we are able to define an equivalence class, we can structure the original set A with respect to this relation.
- Notice that $[a]$ gives a structure to A rather than directly involving the elements from the relation.
- Fix an a, look for all the partner a has; they all belong to the equivalence class.

Lecture 60 - Equivalence Class Examples

Definition

- Consider the relation $\mathcal{R}$ on $\mathbb{Z} \times \mathbb{Z}$ given by

$$(a,b) \sim (c,d) \text{ if and only if } a + d = b + c$$

- Equivalence classes:
  Let $(a,b) \in \mathbb{Z} \times \mathbb{Z}$

$$\begin{aligned}[(a,b)] &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : (a,b) \sim (x,y)\} \\ &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : \begin{array}{l} x \text{ and } y \text{ have the same distance as } a \text{ and } b, \\ \text{and } y \text{ is to the same side of } x \text{ as } b \text{ is to } a \end{array} \}\end{aligned}$$

Lecture 61 - Equivalence Class Example

Example

- Let $\mathcal{R}$ be the equivalence relation on $\mathbb{Z}$ given by $a \sim b$ if and only if a and b have the same parity.

- Let $a \in \mathbb{Z}$. Then $[a] = \{b : b \text{ has the same parity as } a\}$
  (a) a is even: $[a] = \{b : b \text{ is even}\} = 2\mathbb{Z}$
  (b) a is odd: $[a] = \{b : b \text{ is odd}\} = 2\mathbb{Z} + 1$

Content

- The two equivalence class above gives structure to the given sets. We are able to divide $\mathbb{Z}$ into odd and even, justified by the equivalence relation.
- The key is about ***extracting information*** until we get an equivalence relation.

Lecture 62 - Congruences I

Objective:

- **Understand Equivalence classes that come with $\equiv$**
- **Usefulness of modular arithmetic**

Definition

- Let m be a positive integer and let a, b be integers.
  Then

$$a \equiv b \pmod{m} \text{ if and only if } m \mid a - b$$

Exploration

- $\equiv$ is an equivalence relation on $\mathbb{Z}$.
- Given $a \in \mathbb{Z}$.

$$\begin{aligned} [a] = \bar{a} &= \{b \in \mathbb{Z} : a \equiv b \pmod{m}\} \\ a &\equiv \pmod{m} \\ m &\mid a - b \\ mk &= a - b \\ b &= a - mk \\ b &= a + m\tilde{k} \end{aligned}$$

- We can think in terms of the division theorem,

$$0 \leq a < m, b \text{ has remainder } a$$

  which allows us to subdivide $\mathbb{Z}$ into

$$\underbrace{[0], [1], [2], [3], \cdots, [m-1]}_{m \text{ equivalence classes}}$$

Lecture 63 - Congruence II

Proof

- **Theorem**

  (a) For every positive integer m, every integer a is congruent to exactly one element in the set $\{0, 1, 2, \cdots, m-1\} \pmod{m}$.

  (b) $a \equiv b \pmod{m}$ if and only if a and b have the same remainder $\pmod{m}$

  (c) For $a \in \mathbb{Z}, [a] = \{a + km : k \in \mathbb{Z}\}$

- *Proof.*

(a) Let $m \in \mathbb{N}$, let $n \in \mathbb{Z}$.
Division Theorem: There exists unique integers $q, r(0 \leq r < m)$ such that

$$n = q \cdot m + r$$

This means $m \mid n - r$, which gives $n \equiv r \pmod{m}$ and $r \in \{0, 1, \cdots, m-1\}$
Uniqueness: Assume there are $r_1, r_2 \in \{0, 1, \cdots, m-1\}$ such that

$$n \equiv r_1 \pmod{m} \text{ and } n \equiv r_2 \pmod{m}$$
$$m \mid n - r_1 \text{ and } m \mid n - r_2$$
$$m \cdot k_1 + r_1 = n \text{ and } m \cdot k_2 + r_2 = n \text{ for } k_1, k_2 \in \mathbb{Z}$$

But $0 \leq r_1, r_2 < m$, and by the division theorem $r_1 = r_2$.

Lecture 64 - Congruence III

Proof Cont.

Proof. (b) We will prove in both direction $\Rightarrow$ and $\Leftarrow$
$\Rightarrow$ Assume $a \equiv b \pmod{m}$.
Then $m \mid a - b$, so $m \cdot k = a - b$ for some $k \in \mathbb{Z}$.
Thus $a = mk + b$
By the Division Theorem, $b = m \cdot l + r$ for some $l \in \mathbb{Z}$ and $0 \leq r < m$.
Thus by substitution $a = m \cdot k + m \cdot l + r = m(k+l) + r = a$ where $k + l, r \in \mathbb{Z}, 0 \leq r < m$.
By the Division Theorem, r is the remainder of a.
$\Leftarrow$ Let r be the remainder of a and b.
Then $a = m \cdot q_1 + r$ and $b = m \cdot q_2 + r$ by the Division Theorem.
Then $a - b = mq_1 + r - mq_2 - r = m(q_1 - q_2)$
Thus $m \mid a - b$ which means $a \equiv b \pmod{m}$.
(c) Follows directly from (b)

Lecture 65 - Modular Arithmetic

Objective: Explore how $\equiv$ is useful.

Proof

- **Theorem**
  Let $m \in \mathbb{N}$, let $a, b, c, d \in \mathbb{Z}$.
  Assume $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$.

$$a + b \equiv c + d \pmod{m} \tag{4}$$
$$ab \equiv cd \pmod{m} \tag{5}$$

- Notice that for the equations above, taking the modulo before the $+, \cdot$ operation is the same as first reducing with modulo and taking the corresponding operation.
- Such property can be useful in practical applications.

- *Proof.* A direct proof from assumption.
  Show $m \mid a + b - (c + d)$
  Show $m \mid a \cdot b - c \cdot d$ ∎

Lecture 66 - Modular Arithmetic II

Content

- For modulo m, there are only m possible outcomes when we do $+/\cdot$
- Consider modulo 6

•	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- This is called a Multiplication table.
- Note that all entries are from $\{0, 1, 2, 3, 4, 5\}$.
- We present the results in their reduced form.
- Note that the 'old' understanding of $\cdot$ does not hold all the time

$$a \cdot b \equiv 0 \pmod{m} \text{ does not imply } a = 0 \text{ or } b = 0$$
$$2a \equiv 2b \pmod{m} \text{ does not imply } a \equiv b \pmod{m}$$

- With reduced modular prime we will see similar things with the integers again.

Lecture 67 - Modular Arithmetic, the Cool Stuff

Content

- What is $3^{100} \pmod 5$?

$$3^1 \equiv 3 \pmod 5$$
$$3^2 \equiv 4 \pmod 5$$
$$3^3 \equiv 3 \cdot 3^2 \pmod 5$$
$$3^4 \equiv 3^2 \cdot 3^2 \pmod 5$$

- Remember that the equivalence classes are $[0], [1], [2], [3], [4]$
- $[m - 1]$ always contains -1.
- Then we have

$$3^{100} = (3^4)^{25} \equiv (1)^{25} \equiv 1 \pmod 5$$
$$3^{100} = (3^2)^{50} \equiv (-1)^{50} \equiv 1 \pmod 5$$

Lecture 68 - Modular Arithmetic, the Cool Stuff II

Proof

- **Proposition**
  Prove that 11 divides $6^{123} - 7$
- *Proof.*

$$\begin{aligned} 6 &\equiv 6 \pmod{11} \\ 6^2 &\equiv 3 \pmod{11} \\ 6^3 \equiv 6 \cdot 6^2 &\equiv 18 \equiv 7 \pmod{11} \\ 6^4 \equiv 6^2 \cdot 6^2 &\equiv 3 \cdot 3 \equiv 9 \pmod{11} \\ 6^5 &\equiv 21 \equiv 10 \equiv (-1) \pmod{11} \\ 6^{123} = (6^5)^{24} \cdot 6^3 &\equiv (-1)^{24} \cdot 7 \equiv 7 \pmod{11} \end{aligned}$$

  Therefore $6^{123} - 7 \equiv 7 - 7 \equiv 0 \pmod{11}$.
  Thus $11 \mid 6^{123} - 7$. ∎

Lecture 69 - Modular Arithmetic Proofs

Proof

- **Theorem**
  $3 \mid x \iff 3 \mid x^3$
- *Proof.* We will use congruence to prove this.

  $\Rightarrow$ is clear.
  $\Leftarrow$

$[x]$	0	1	2	(mod 3)
$[x^3]$	0	1	2	

  We see in the table that

$$x^3 \equiv 0 \pmod{3} \text{ if and only if } x \equiv 0 \pmod{3}$$

  If $3 \mid x^3$ then $3 \mid x$. ∎
- Remember the key observation: If $m \mid z$ then $z \equiv 0 \pmod{m}$. Then $m \cdot k = z$, thus $m \cdot k \equiv 0 \pmod{z}$.

Lecture 70 - Modular Arithmetic and Proofs II

Proof

- **Theorem**
  If a, b are odd integers, there is no c such that $a^2 + b^2 = c^2$.
- *Proof.* We want to check that whether $a^2 + b^2 \mid c^2$. Let a, b be odd integers.
  Then modulo 4.

a	1	3	(mod 4)
a^2	1	1	

Same table for b.

a^2+b^2	1	(a^2)	(mod 4)
1	2		
b^2			

Then we see the table for c^2

c	0	1	2	3	(mod 4)
c^2	0	1	0	1	

This table shows that c^2 can never be equal to a^2+b^2 when a, b are odd. ■

Lecture 71 - Modular Arithmetic and Proofs

Objective: Modulo and Proofs, digits and Mod

Example

- $\underbrace{1}_{10^4}\underbrace{7}_{10^3}\underbrace{0}_{10^2}\underbrace{7}_{10^1}\underbrace{2}_{10^0} = 1\cdot 10^4 + 7\cdot 10^3 + 0\cdot 10^2 + 7\cdot 10^1 + 2\cdot 1$
- $\pmod{10} : 2$
- $\pmod{100} : 72$
- Remember to use the theorem

$$\text{If } a \equiv c \pmod{m}, b \equiv c \pmod{m} \text{ then } a+b \equiv c+d \pmod{m}.$$

Lecture 72 - Modular Arithmetic and Digits

Proof

- **Theorem**
  Let n be a positive integer and let s be the sum of the digits of n.
  Then
  $$n \equiv s \pmod{9}$$
- *Proof.* Let $k \geq 0, k \in \mathbb{Z}$. Let $a_0, \cdots, a_k$ be integers.
  Then
  $$\sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \pmod{9}$$
  - By Induction.
  - Base case: $k = 0, \sum_{i=0}^{0} a_i \cdot 10^i = a_0 \cdot 10^0 = a_0 = \sum_{i=0}^{0} a_i \pmod{9}$
  - IH: Let $l = 0$ and assume
  $$\sum_{i=0}^{l} a_i \cdot 10^i \equiv \sum_{i=0}^{l} a_i \pmod{9} \tag{6}$$

– Induction Step: Note that $10^{l+1} \equiv 1 \pmod 9$. Then we have

$$\underbrace{99\cdots9}_{l}+1 \equiv 1 \pmod 9$$

$$\sum_{i=0}^{l+1} a_i \cdot 10^i = a_{l+1} \cdot 10^{l+1} + \sum_{i=0}^{l} a_i \cdot 10^i \equiv 1 \pmod 9$$

$$a_{l+1} + \sum_{i=0}^{l} a_i \equiv \sum_{i=0}^{l+1} a_i \pmod 9$$

Thus, by the PMI, 6 holds. ∎

Lecture 73 - Functions

Objective: Define Functions

Definition

- Let A, B be sets. Then a function from A to B is a relation $\underbrace{\text{from } A \text{ to } B}_{\subseteq A \times B}$ such that

  For each $a \in A$ there exists $b \in B$ such that $(a, b) \in f$.
  For each $a \in A$ there exists a unique $b \in B$ such that $(a, b) \in f$.

  Such a function is denoted by $f : A \to B$.
  The set A is the domain of f, the set B is the codomain of f.
- $f : \mathbb{R} \to \mathbb{R}, f = \{(x, x^2)\}$.
- The range of f is the collection/set of all outputs:

$$\text{range } f = \{b \in B : \text{there is } a \in A \text{ with } (a, b)\} \subseteq B$$

- Note: In the 18/19 century, the notation is $f(x) = x^3 + 2x + \ln x$.
  We take the set theory approach through relation: $(x, x^3 + 2x + \ln x)$.
  In general:

$$(a, b) \in f \iff f(a) = b$$
$$(a, f(a)) \iff f(a) = b$$

Zhewen Zheng
University of Washington

Removed excessive examples.

Lecture 74 - Functions, Examples

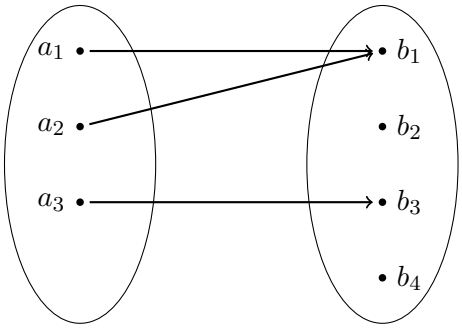
Content

- Function is a machine. As the operator we need to feed it elements from the domain, and make sure that the choice of domain allows the function to evaluate every single element.
- The function must be design to have ***exactly one output***.

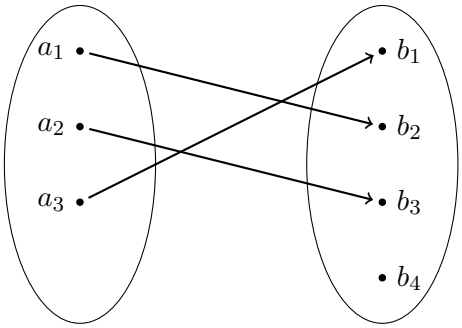
Lecture 75 - Injective, Surjective, Bijective

Definition

- Let $f : A \to B$ be a function.
  (a) f is **injective** (one to one)
  SCHEME: If $f(a_1) = f(a_2)$ then $a_1 = a_2$. (**OR**: If $a_1 \neq a_2$ then $f(a_1) \neq f(a_2)$)
  (b) f is **surjective** (onto) if range $f = B$
  SCHEME: If $b \in B$ then there is $a \in A$ such that $f(a) = b$.
  (c) f is **bijective** if it is injective and surjective.



(a) Not injective, Not surjective



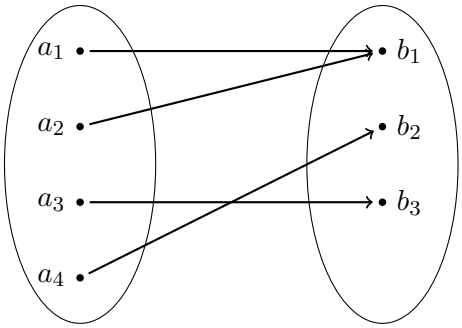
(b) Injective, Not surjective

Lecture 76 - Injective, Surjective, Examples

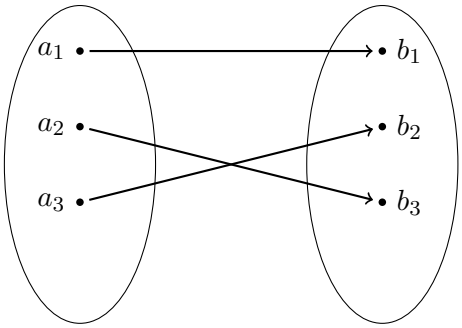
Example

(a) $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2 + 1$

(b) $f : \mathbb{Z} \to \mathbb{Z}, f(x) = 5x - 7$



(a) Not injective, Surjective



(b) Injective, Surjective

(c) $f : \mathbb{Z} \to \mathbb{Z}, f(x) = \begin{cases} x+2 & x \text{ is even} \\ x-6 & x \text{ is odd} \end{cases}$

x	0	1	2	3	4	5	6
$f(x)$	2	-5	4	-3	6	-1	8

If x is even, then $f(x)$ is even. $(x = 2k, f(x) = 2(k+1))$.
If x is odd, then $f(x)$ is odd. $(x = 2k+1, f(x) = 2(k-3)+1)$.

Lecture 77 - Injective, Surjective, Examples II

Example Cont.

(c) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, f((m,n)) = (m+n, 2m+n)$

Lecture 78 - Compositions

Definition

(a) Let A be a set. Consider $f : A \to A, f(a) = a, [\{(a,a) : a \in A\} = f]$.
f is called ***identity function*** on A, denoted by id_A.

(b) Let A, B be sets, let $b \in B$, let $b \in B$.
Consider $f : A \to B$ with $f(a) = b$ for all $a \in A, [\{(a,b) : a \in A\}]$
f is called constant function.

(c) Let A, B, C be sets. Let $f : A \to B, g : B \to C$ be functions.
The composition of g with f, denoted by $g \circ f$ is defined by

$$g \circ f = \{(a,c) : a \in A, c \in C \text{ and } c = g(f(a))\}$$

Lecture 79 - Compositions are functions

Objective: $g \circ f$ is a function

Proof

- **Theorem**
If $f : A \to B, g : B \to C$ are functions then $g \circ f$ is a function.

- *Proof.* Let $a \in A$.
  Then there is a unique $f(a) \in B$. (f is a function).
  Then there is a unique $g(f(a)) \in C$. (g is a function).
  Thus given a, there is a unique $c \in C$ such that $g \circ f(a) = c$. ∎

Lecture 80 - Properties of compositions I

Objective: Properties of composite functions

Proof

- **Theorem**
  Let A, B, C be sets. Suppose $f : A \to B, g : B \to C$ are injective functions.
  Then $g \circ f$ is an injective function from A to C.
- *Proof.* Let $a, b \in A$ such that $g \circ f(a) = g \circ f(b) \iff g(\underbrace{f(a)}_{\in B}) = g(\underbrace{f(b)}_{\in B})$.
  We know that g is injective by hypothesis. Therefore $f(a) = f(b)$.
  Now, f is also injective. Thus $a = b$. ∎

Lecture 81 - Properties of compositions II

Objective: Properties Compositions: Given property of $g \circ f$, what do we know about g, f

Proof

- **Theorem**
  Let A, B, C be sets, $f : A \to B, g : B \to C$ functions.

  (a) If $g \circ f$ is injective then f is injective.

  (b) If $g \circ f$ is injective then g is not necessarily injective.

  (c) If $g \circ f$ is surjective then g is injective.

  (d) If $g \circ f$ is surjective then f is not necessarily surjective.

Lecture 82 - Inverse Relations

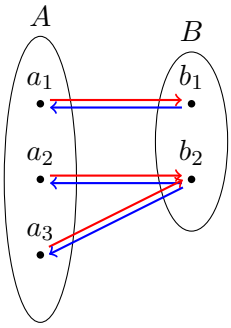
Objective: Defined Inverse Relations

Definition

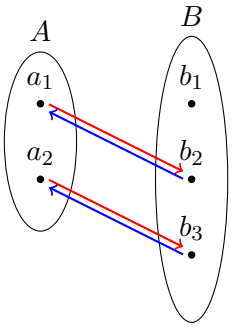
- Let A, B be sets and let R be a relation from A to B. ($R \subseteq A \times B$)
- The inverse R^{-1} of R is the relation from B to A defined as

$$R^{-1} = \{(b, a) : (a, b) \in R\}$$

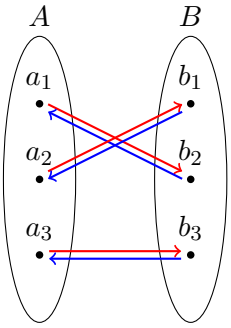
- These are not functions yet!



(a) Not Injective, Surjective.



(b) Injective, Not Surjective



(c) Injective, Surjective.

Lecture 83 - Inverse Functions

Objective: When are inverse relations also functions?

Example

- Figure 1: b_2 has 2 outputs for f^{-1}. So f^{-1} is not a function as f was not injective.
- Figure 2: b_1, b_4 do not have an output for g^{-1}. So g^{-1} is not a function as g was not surjective.
- Figure 3: h^{-1} is a function.
- Through examples we get a hint of the criteria: inverse relations seems to be functions only when the relation is ***bijective***.

Lecture 84 - Inverse Functions II

Objective: State and prove the theorem about inverse relations being functions.

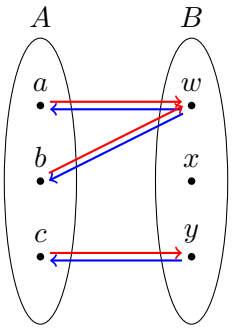


Figure 4: Not injective, Not surjective.

Proof

- **Theorem**
  Let A, B be sets. Suppose $f : A \to B$ is a function.
  Then f^{-1} is a function if and only if f is bijective.
- *Proof.* $f : A \to B. f^{-1} : B \to A$.

$\Leftarrow$ Assume f is bijective.
Let $b \in B$. Show there exists a unique $a \in A$ such that $(b, a) \in f^{-1}$.
Clue: use the fact that f is bijective to prove the existence and uniqueness of a

$\Rightarrow$ Assume $f : A \to B, f^{-1} : B \to A$ are both functions.
Clue: use the fact that f, f^{-1} are functions to prove the bijectivity of f. ■

Lecture 85 - Inverse Functions III

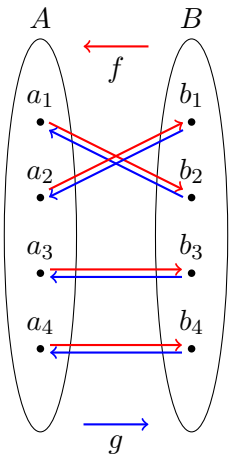
Objective: Find out how a function and its inverse "work" together.

Proof

- **Theorem**
  Let A, B be sets. Let $\mathrm{id}_A, \mathrm{id}_B$ be the respective identity functions on A, B.
  Suppose $f : A \to B$ and $g : B \to A$ are functions such that

$$\underbrace{g \circ f}_{\text{domain } A} = \mathrm{id}_A \text{ and } \underbrace{f \circ g}_{\text{domain } B} = \mathrm{id}_B$$

  Then $g = f^{-1}$ and $f = g^{-1}$. In particular, f, g are bijective.



- Note: If $f : A \to B$ is given and you are able to find a function $g : B \to A$ such that $f \circ g = \mathrm{id}_B, g \circ f = \mathrm{id}_A$, then you don't need to check/confirm bijectivity of f or g.

Lecture 86 - Inverse Functions IV

Objective: Proof following last lecture.

Proof

- *Proof.* We will show that $g = f^{-1}$. The statement $f = g^{-1}$ will go likewise.
  Clue: understand g, f^{-1} as subsets of $B \times A$ and show set equality through $\subseteq$ and $\supseteq$. ■

Lecture 87 - Examples of Inverses I

Example

- $f : \mathbb{R} \to \mathbb{R}^{\geq 0}, f(x) = x^2$
  $g : \mathbb{R}^{\geq 0} \to \mathbb{R}, g(x) = \sqrt{x}$
  Then $f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x = \mathrm{id}_{\mathbb{R}^{\geq 0}}(x)$.
  But: $g(f(-1)) = g((-1)^2) = g(1) = \sqrt{1} = 1 \neq -1$.
  Not enough to just check $f \circ g = \mathrm{id}_B$. We must always check both $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$, too.

Lecture 88- Examples of Inverses II

Example

- Let $a, b \in \mathbb{R}, a \neq 0$. Consider $f : \mathbb{R} \to \mathbb{R}, f(x) = ax + b$ for all $x \in \mathbb{R}$.
  Find the inverse function.
  Clue: solve for x and switch the variables x, y. Find the inverse $g(x)$, and then verify that it is true by checking that $g \circ f$ and $f \circ g$ equal to their corresponding identity functions.

Lecture 89 - Examples of Inverse III

Example

- Consider $f : \mathbb{R} \setminus \{-\frac{4}{3}\} \to \mathbb{R} \setminus \{0\}, f(x) = \frac{1}{3x+4}$
  Find f^{-1}.
  Claim: $g : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{-\frac{4}{3}\}$

$$g(x) = \frac{1}{3x} - \frac{4}{3}$$

  Verify that it is true by checking that $g \circ f$ and $f \circ g$ equal to their corresponding identity functions.

Lecture 90 - Examples of Inverses IV

Example

- Consider $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, f(m, n) = (\underbrace{5m + 4n}_{y}, \underbrace{4m + 3n}_{z})$.
  Find the inverse.
- Remember: We are mapping pairs, and we need to solve a system of linear equations for m, n. Do that on the scratch paper.
- Claim: $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$

$$g(y, z) = (-3y + 4z, 4y - 6z)$$

  is the inverse of f.
  Verify that it is true by checking that $g \circ f$ and $f \circ g$ equal to their corresponding identity functions.

Zhewen Zheng
University of Washington

Lecture 91 - Image and Pre-Image

Objective: Introduce Image and Pre-Image

Definition

- Let $f : A \to B$ be a function
  (a) If $X \subseteq A$, the image of X is the set $f(X) = \{f(x) : x \in X\} \subseteq B$
  (b) If $Y \subseteq B$, the pre-image of Y is the set $f^{-1}(Y) = \{x \in A : f(x) \in Y\} \subseteq A$.
- Remember we are applying f to a set to obtain the image (which is also a set).
- $f^{-1}(Y)$ ***exists even if*** f ***is not invertible***; f^{-1} of a set is to find pre-images that maps into the given set Y. The argument for pre-image is a set, not an element, which differs from what we meant by ***inverse***. See examples below for demonstration.

Example

- Let A, B be nonempty sets and let $f : A \to B$ be a function, $X \subseteq A, Y \subseteq B$. The following are true:
  (a) $f^{-1}(Y)$ can be the empty set.
  (b) $f(X) \subseteq B$. ($f(A) = \text{range} f$ by definition.)
  (c) $f^{-1}(Y) \subseteq A$ ($f^{-1}(B) = A$ when the f is surjective. Otherwise we only have $\subseteq$)

Lecture 92 - Image and Pre-Image II

Proof

- **Theorem**
  Let $f : A \to B, X \leq A, Y \subseteq B$.
  (a) $X \subseteq f^{-1}(f(X))$
  (b) $f(f^{-1}(Y)) \subseteq Y$.
- For an X mapping into $f(X)$, it is possible to get elements that were not from X, but still mapped into $f(X)$, out of $f^{-1}(f(X))$.
- Similarly, elements in $f^{-1}(Y)$ that does not necessarily map to all elements of Y.

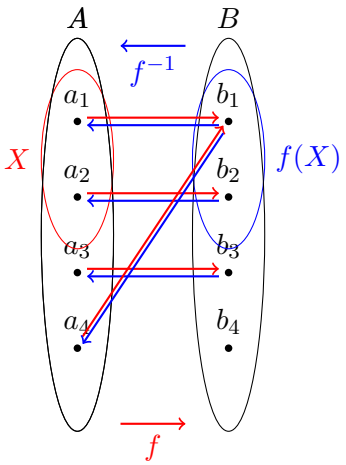


Figure 5: Yes, tikz used here.

Lecture 93 - Equinumerous

Objective: Define Equinumerousity

- This chapter is a big application of ***bijective functions***.

Definition

- Let A, B be sets. Then we say A, B are equinumerous

$$A \sim B$$

  if there is a bijection $f : A \to B$.
- It is equivalent to say there is a bijection $g : B \to A$ (they are inverses of each other); though, sometimes proving bijection from one side is easier.

Example

- For proving $A \sim B$, construct a way of having a bijective mapping between A and B.
- Let $A = \{1, 2, 3, 4\}, C = \{1, 2\}$. Then $A \nsim C$.

  Proof. If $f : A \to C$ was a bijection, then g would be injective.
  A has 4 distinct elements, so $g(A)$ must also have at least 4 elements, which cannot happen since C only has 3. ∎

Lecture 94 - $\mathbb{Z}$ and $2\mathbb{Z}$ are equinumerous

Objective: Show $\mathbb{Z} \sim 2\mathbb{Z}$

Example

- Let $2\mathbb{Z}$ be the set of all even numbers. Then $\mathbb{Z} \sim 2\mathbb{Z}$.

- Show $f : \mathbb{Z} \to 2\mathbb{Z}, f(x) = 2(x)$ then f is bijective.
- Show injectivity, surjectivity with the usual scheme. Refer back to the ***injective and surjective lectures***.

Lecture 95 - Finite Sets, Cardinality

.

Objective: Define finite, infinite, and cardinality

- $\mathbb{Z} \sim 2\mathbb{Z}$ is a different matter to $2\mathbb{Z} \subseteq \mathbb{Z}$.

Definition

- Let S be a set. Then S is ***finite*** if
  (a) $S = \emptyset$ **OR**
  (b) If there exists a bijection f from $S \to \{1, \cdots, n\}, n \in \mathbb{N}(S \sim \mathbb{N})$.
  (c) In this case we say S has cardinality n. $(|S| = n)$
- If S is not finite, it is ***infinite***.
- Note: very common: $|\emptyset| = 0$, if S infinite: $|S| = \infty$ (Not for our text).

Lecture 96 - Subsets of $\mathbb{N}$ are finite

Objective: Prove that subsets of finite sets are finite

Proof

- **Theorem**
  Let $n \in \mathbb{N}$. Then all subsets of $\{1, \cdots, n\}$ are finite.

  Proof. We use induction on n.
  Let $I_c = \{1, \cdots, c\}, P(n) =$ all subsets of $\{1, \cdots, n\} = I_n$ are finite.
  - Base Case: $n = 1$. Then $I_1 = \{1\}$. Then $\emptyset, I$ are the only subsets of I_1.
    $\emptyset$ is finite by def.
    $\mathrm{id}_{I_1} : I_1 \to I_1$ is a bijection from $\{1\} \to \{1\}$.
    Thus for $n = 1$ the statement holds.
  - IH: Assume $P(k)$ is true for ***some*** $k \geq 1$.
  - Induction Step: Consider $I_{k+1} = \{1, 2, \cdots, k, k+1\}$
    Let $S \subseteq I_{k+1}$.
    Use $S = T \cup \{k+1\}$. Prove by cases of $k+1 \notin S$ and $k+1 \in S, T = \emptyset, T \neq \emptyset$.
    Find a function and use definitions of injectivity, surjectivity, bijectivity, and finite. ∎

Lecture 97 - Equinumerosity is an Equivalence Relation

Objective: Prove that $\sim$ is an equivalence relation

Proof

- **Theorem**
  Let $\mathcal{F}$ be a family. Then the relation R on $\mathcal{F}$ ($R \subseteq F \times F$) defined by

  $$(A, B) \in R \text{ if and only if } A \sim B$$

  is an equivalence relation.

  Proof. (R) Let $A \in R$. Then $\underbrace{\mathrm{id}_A : A \to A}_{\mathrm{id}(a)=a}$.
  (S) Let $(A, B) \in R$. Then $A \sim B$.

  $$f \circ f^{-1} = \mathrm{id}_B \text{ and } f^{-1} \circ f = \mathrm{id}_A \Rightarrow (f^{-1})^{-1} = f$$

  Thus $B \sim A$.
  (T) Let $(A, B), (B, C) \in R$. Then $A \sim B, B \sim C$.

  $$f : A \to B, g : A \to C \Rightarrow g \circ f : A \to C \text{ is a bijection.}$$ ∎

Lecture 98 - Countable Sets

Objective: Introduce Countable Sets

Definition

- A set is ***countable*** if it is finite ($\emptyset$ or $\sim \{1, \cdots, n\}$) or equinumerous to $\mathbb{N}$.
- A set that is infinite and countable is called ***countably infinite***.

Lecture 99 - $\mathbb{Z}$ is Countable

Objective: Prove $\mathbb{Z}$ is Countable

Example

- This proof gives a scheme to how these proofs work.
- We want to establish a bijection $f : \mathbb{N} \to \mathbb{Z}, g : \mathbb{Z} \to \mathbb{N}$.

Proof

- $\mathbb{Z}$ is countable.

  Proof. $g : \mathbb{Z} \to \mathbb{N}, g(x) = \begin{cases} 2x & x > 0 \\ 1 - 2x & x \leq 0 \end{cases}$
  Claim g is bijective.
  Consider $f : \mathbb{N} \to \mathbb{Z}, f(x) = \begin{cases} \frac{1}{2}x & x \text{ even} \\ \frac{1-x}{2} & x \text{ odd} \end{cases}$.
  Clue: Map evens to $\{0, 1, \cdots, n\}$, odds to $\{-1, -2 \cdots, -n\}$.
  Use the usual $g \circ f = \mathrm{id}_{\mathbb{N}}, f \circ g = \mathrm{id}_{\mathbb{Z}}$ to show that they are inverses and it is a bijection. ∎

Lecture 100 - Subsets of $\mathbb{N}$ are Countable

Objective: Subsets of $\mathbb{N}$ are countable

Proof

- **Theorem**
  Let $A \subseteq \mathbb{N}$. Then A is countable.

  Proof. Let $A \subseteq \mathbb{N}$.
  - If A is finite then we are done.
  - Assume that A is infinite. Since $A \subseteq \mathbb{N}$, the ***Well Ordering Principle*** guarantees the existence of a smallest element a_1.
  - Well Ordering Principle provides a rule for us to ***select elements***.
  - Define $f : A \to \mathbb{N}, f(a_1) = 1$.
    Consider $A \setminus \{a_1\}$, an infinite subset of $\mathbb{N}$.
    Use Well Ordering Principle to select the smallest element again;
    $\vdots$
    $f : A \to \mathbb{N}, f(a) = i$, where $a = a_i$, all a_i's are distinct. Thus f is injective.
    Since A is infinite, for all $k \in \mathbb{N}$ there is a_k such that $f(a_k) = k$.
    f is a bijection, $A \sim \mathbb{N}$. ∎

Lecture 101 - Subsets of Countable sets are Countable

Objective: Same as title.

Note: Most proofs this week are brilliant. I wanted to include more detail because some clues might not be sufficient.

Proof

- **Theorem**
  Subsets of countable sets are countable.

  Proof. Let A be a countable set. Let $B \subseteq A$.

  (a) B finite $\to B$ is countable.

  (b) Let B be infinite.

  (c) We find $g : B \to K, g(b) = f(b)$. (Restrict f's domain to B)
  - g is injective because f is injective.
  - g is surjective because we defined K as both the codomain and range.

  Since $K \subseteq \mathbb{N}$, K is countable, $K \sim \mathbb{N}$.
  By g, $B \sim K$, so $B \sim \mathbb{N}$. ∎

Lecture 102 - Union of Two Finite Sets is Finite

Proof

- **Theorem**
  The union of two finite sets is finite.

  Proof. Proved in HW7, $|A \cup B| = |A| + |B| - |A \cap B|$ is a finite number. ∎

Lecture 103 - Unions of Countable Sets

Objective: Generalize about unions of Countable Sets

Proof

- **Theorem**
  Let A be a finite set, B be a countable infinite set.
  Suppose $A \cap B = \emptyset$, then $A \cup B$ is countable infinite.

  Proof. Let A be finite, B be countable infinite, $A \cap B = \emptyset$.

  (a) $A = \emptyset$. Then $A \cup B = B$, which is countable infinite.

(b) Let $A \neq \emptyset$, so $|A| = n, n \geq 1$.
There is a bijection $f : A \to \{1, \cdots, n\}$.
There is a bijection $g : B \to \mathbb{N}$.

(c) We need to fine a bijection $A \cup B \to \mathbb{N}$.
Consider $h : A \cup B \to \mathbb{N}, h(x) = \begin{cases} f(x) & x \in A \\ g(x) + n & x \in B \end{cases}$.

- For surjectivity, consider a $m \in \mathbb{N}$ by choice and show surjectivity in both cases $1 \leq m \leq n$ and $n < m$.
- For injectivity, show that if $h(x_1) = h(x_2)$ then $x_1 = x_2$ in both cases $1 \leq h(x_1) \leq n$ and $n < h(x_1)$.

Thus bijectivity of h is shown. ∎

Lecture 104 - Unions of Countable Sets II

Objective: Continue to investigate unions of countable sets

Proof

- **Theorem**
The union of two disjoint infinite countable sets is countable.

Proof. Let A, B be countable infinite sets, $A \cap B = \emptyset$.
Then there is a bijection $f : A \to \mathbb{N}, g : B \to \mathbb{N}$.
We want a bijection $A \cup B \to \mathbb{N}$.
Define $h : A \cup B \to \mathbb{N}, h(x) = \begin{cases} 2f(x) - 1 & x \in A \\ 2g(x) & x \in B \end{cases}$.

- Injective: show $h(x_1) = h(x_2)$ on both even and odd cases.
- Surjective: f runs through all $n \in \mathbb{N}$, $2f - 1$ runs through all odd positives.
g runs through all $n \in \mathbb{N}$, $2g$ runs through all even naturals. ∎

Lecture 105 - Unions of Countable Sets III

Objective: Unions of general infinite countable sets

Proof

- **Theorem**
The union of two countable infinite sets is countable infinite.

Proof.

$$A \cup B = \underbrace{(A \setminus B)}_{1} \cup \underbrace{(A \cap B)}_{2} \cup \underbrace{(B \setminus A)}_{3}$$

where $1, 2, 3$ are pairwise disjoint.

(a) $A \setminus B \subseteq A \to A \setminus B$ finite or countable infinite

(b) $A \cap B \subseteq A \to A \cap B$ finite or countable infinite

(c) $B \setminus A \subseteq B \to B \setminus A$ finite or countable infinite

Then $(A \setminus B) \cup (A \cap B)$ is either finite or countable infinite.
Then $[(A \setminus B) \cup (A \cap B)] \cup (B \setminus A)$ not finite but countable infinite. ■

Lecture 106 - $\mathbb{N} \times \mathbb{N}$ is countable

Objective: Prove $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ is countable.

Proof

- **Theorem**

$$\mathbb{N} \times \mathbb{N} \sim \mathbb{N} \text{ i.e. } \mathbb{N}^2 \text{ is countable infinite.}$$

Proof.

$\mathbb{N}/\mathbb{N}$	1	2	3	4	5	$6 \cdots$
1	1	3	6	10	15	$\cdots$
2	2	5	9	14		$\cdots$
3	4	8	13			$\cdots$
4	7	12				$\cdots$
5	11					$\cdots$
6						$\cdots$
$\vdots$						

Consider a function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, f((i,j) = j + \frac{1}{2}(i+j-2)(i+j-1)$ on the diagonal of the table. This gives a injective and surjective mapping between $\mathbb{N}$ and all pairs in $\mathbb{N} \times \mathbb{N}$. ■

Lecture 107 - $\mathbb{Q}+$ is countable

Objective: Prove $\mathbb{Q}_{>0}$ is countable

- **Theorem**
  The set of positive rational number $\mathbb{Q}_{>0}$ is countable infinite.

  Proof. Let $x \in \mathbb{Q}_{>0}$. Then we can find $a, b \in \mathbb{N}$ such that a, b have ***no common divisors except for 1***, such that $x = \frac{a}{b}$.
  Define

$$g : \mathbb{Q}_{>0} \to \mathbb{N} \times \mathbb{N}$$
$$g(x) = (a,b) \text{ where } x = \frac{a}{b} \text{ as above.}$$

  Note: g is not surjective; $g(x) \neq (10, 20)$.
  Then $\text{range}(g) = C \subsetneq \mathbb{N} \times \mathbb{N}$.
  Then $g : \mathbb{Q}_{>0} \to C$ is bijective.

$$g(x_1) = g(x_2) \Leftrightarrow (a_1, b_1) = (a_2, b_2) \Leftrightarrow \frac{a_1}{b_1} = \frac{a_2}{b_2}$$

Thus g is injective.
Then $\mathbb{Q}_{>0} \sim C \subseteq \mathbb{N} \times \mathbb{N}$.
Then

$$C \sim \mathbb{N}, C \sim \mathbb{Q}_{>0}$$

so $\mathbb{Q}_{>0} \sim \mathbb{N}$ and thus is countable. ■

- Notice that we made g which originally was not bijective into a bijective function by modifying the codomain.
- We can try to utilize the transitivity of equinumerous equivalence relation; showing something is equinumerous as a subset of $\mathbb{N}$, or something that we have proved to be equinumerous to $\mathbb{N}$ is sufficient to prove its countable.

Lecture 108 - $\mathbb{Q}$ is countable

Objective: Prove $\mathbb{Q}$ is countable

Proof

- Our previous preparations finally brings us the ease in proving this theorem.
- **Theorem**
  $\mathbb{Q}$ is countable.

  Proof. $\mathbb{Q}_{>0}$ is countable.
  $\mathbb{Q}_{>0} \to \mathbb{Q}_{<0}, h(x) = -x$ is a bijection.
  Thus $\mathbb{Q}_{>0} \sim \mathbb{Q}_{<0}, \mathbb{Q}_{<0}$ is countable.
  $\mathbb{Q} = \mathbb{Q}_{>0} \dot{\cup} \mathbb{Q}_{<0} \dot{\cup} \{0\}$.
  The union of two countable infinite set is countable ($\mathbb{Q}_{>0}$ and $\mathbb{Q}_{<0}$);
  The union of a countable infinite set with a finite set is still countable ($\mathbb{Q}_{>0} \dot{\cup} \mathbb{Q}_{<0}$ and $\{0\}$);
  Therefore, $\mathbb{Q}$ is countable.

Lecture 109 - $\{0, 1\}$ and $\mathbb{R}$ are equinumerous.

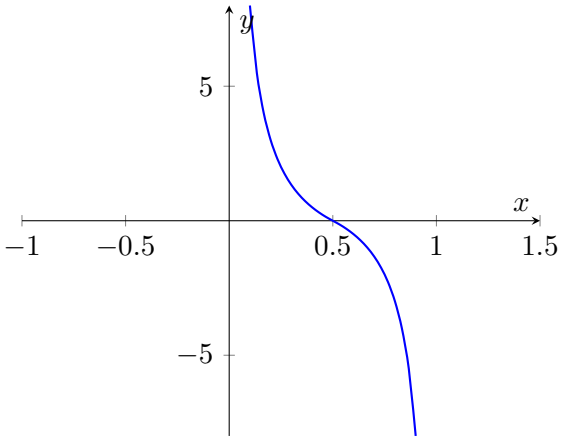
Objective: Show $\mathbb{R}$ is not countable (see title.)

- **Theorem**
  The real interval $(0, 1)$ and $\mathbb{R}$ are equinumerous.

  Proof. Consider

  $$f : (0,1) \to \mathbb{R}, f(x) = \begin{cases} \frac{1}{x} - 2 & 0 < x \leq \frac{1}{2} \\ 2 - \frac{1}{1-x} & \frac{1}{2} < x < 1 \end{cases}$$

  – Notice that f is strictly decreasing, range$f = \mathbb{R} = (-\infty, \infty)$.



– Consider

$$g(x) = \begin{cases} \frac{1}{x+2} & x \geq 0 \\ 1 + \frac{1}{x-2} & x < 0 \end{cases}$$

If $x \geq 0$ then $g(x) = \frac{1}{x+2}, 0 < g(x) \leq \frac{1}{2}$
If $x < 0$ then $g(x) = 1 + \frac{1}{x-2}, \frac{1}{2} < g(x) < 1$
Thus $g : \mathbb{R} \to (0, 1)$.
If $0 < x \leq \frac{1}{2}$ for f, $x \geq 0$ for g

$$f \circ g = f\left(\frac{1}{x+2}\right) = \frac{1}{\frac{1}{x+2}} - 2 = x$$
$$g \circ f = g\left(\frac{1}{x} - 2\right) = \frac{1}{\frac{1}{x} - 2 + 2} = x$$

If $\frac{1}{2} < x < 1$ for f, $x > 0$ for g

$$f \circ g = f\left(1 + \frac{1}{x-2}\right) = 2 - \frac{1}{1 - \left(1 + \frac{1}{x-2}\right)} = x$$
$$g \circ f = g\left(2 - \frac{1}{1-x}\right) = 1 + \frac{1}{2 - \frac{1}{1-x} - 2} = x$$

Lecture 110 - $\mathbb{R}$ is not countable

Objective: Prove $\mathbb{R}$ is not countable.

Content

- Back in 1891 we had Cantor who did this proof.
- He used the ingenious and innovative ***Diagonal Argument***.

Proof

- **Theorem**
  The set of real numbers is uncountable.

  Proof. We will show that $(0,1)$ is uncountable.
  Let $f : \mathbb{N} \to (0,1)$ be a function.
  Let $x \in (0,1)$, we write x in its decimal expansion with finitely many decimal places.

n	$f(a)$
1	$0.a_{1,1}a_{1,2}a_{1,3}a_{1,4}\cdots$
2	$0.a_{2,1}a_{2,2}a_{2,3}a_{2,4}\cdots$
3	$0.a_{3,1}a_{3,2}a_{3,3}a_{3,4}\cdots$
4	$0.a_{4,1}a_{4,2}a_{4,3}a_{4,4}\cdots$
5	$0.a_{5,1}a_{5,2}a_{5,3}a_{5,4}\cdots$
$\vdots$	

  Consider the diagonal of the table. We are trying to devise a number in $(0,1)$ that is not in the table.
  Consider $d = 0.d_1d_2d_3d_4d_5\cdots$ where

$$d_i = \begin{cases} 1 & a_{i,1} \neq 1 \\ 2 & a_{i,1} = 1 \end{cases}$$

  (a) We see that $0 < d < 1, d_i \in \{1,2\}$ and $d \neq f(a_i)$ since d differs with $f(a_i)$ on diagonal entry $(a_{i,i})$ by construction.

  (b) Thus, f is not surjective since d is not in range$f$.

  (c) Therefore f is not bijective and $\mathbb{R} \nsim \mathbb{N}$.

  (d) Thus $\mathbb{R}$ is uncountable. ∎

Lecture 111 - $\mathbb{R} \setminus \mathbb{N}$ not countable

Proof

- **Corollory**
  $\mathbb{R} \setminus \mathbb{N}, \mathbb{R} \setminus \mathbb{Q}$ not countable.

  Proof.

$$\mathbb{R} = \mathbb{R} \setminus \mathbb{N} \dot{\cup} \mathbb{N}$$

  If $\mathbb{R} \setminus \mathbb{N}$ were countable, then the above would be countable too.
  Then $\mathbb{R}$ would be countable, which is a contradiction.
  Thus $\mathbb{R} \setminus \mathbb{N}$ is not countable.
  $\mathbb{R} \setminus \mathbb{Q}$ is proven in the same manner. ∎

Zhewen Zheng
University of Washington

Problem 1:

(a) Let x and y be positive real numbers. Write the contrapositive of the following statement.
If $\sqrt{xy} \neq \frac{x+y}{2}$ then $x \neq y$.

(b) Prove the following theorem, using part (a)
Theorem Let x, y be positive real numbers. If $\sqrt{xy} \neq \frac{x+y}{2}$, then $x \neq y$.

Problem 2:
Let a, b be integers. Prove that $|a \cdot b| = |a| \cdot |b|$.

Solution:

(a) The contrapositive is the following:
If **NOT** $(x \neq y)$ then **NOT** $(\sqrt{xy} = \frac{x+y}{2})$
If $x = y$ then $\sqrt{xy} = \frac{x+y}{2}$

(b) We prove the above statement by proving its contrapositive.
Lets assume $x, y \in \mathbb{R}, x > 0, y > 0$ .By closure and reflexivity we have

$$\sqrt{xy} = \sqrt{xy}$$

Then by substitution we have

$$\sqrt{xy} = \sqrt{x \cdot x} = |x|$$

Since $x > 0$, $|x| = x$. Thus we have

$$\sqrt{x \cdot x} = x$$

We have $1 = 2 \cdot \frac{1}{2}$, and substitute it into the multiplicative identity $x = 1 \cdot x$ we have

$$x = (2 \cdot \frac{1}{2}) \cdot x$$

By commutativity and associativity we have

$$(2 \cdot \frac{1}{2}) \cdot x = \frac{1}{2} \cdot (2 \cdot x) = \frac{x + x}{2}$$

Finally, by substitution we obtain

$$\sqrt{xy} = \frac{x + x}{2} = \frac{x + y}{2}$$

Solution: Let $a, b \in \mathbb{Z}$.
First case: a is positive, b is positive. Then, by the definition of positive,

$$a > 0, b > 0$$

By definition of absolute value and positive closure we have

$$|a| = a, |b| = b, |ab| = ab$$

Using substitution we obtain

$$|ab| = |a| \cdot |b|$$

Second case: a is negative, b is negative. Then, by the definition of negative,

$$a < 0, b < 0$$

By the additive inverse we know

$$a + (-a) = 0, b + (-b) = 0$$

where $(-a)$ and $(-b)$ are positive. Using Part II of the EPI, we have

$$(-a) \cdot (-b) = ab$$

hence by substitution and definition of absolute value

$$|ab| = |(-a) \cdot (-b)| = (-a) \cdot (-b)$$

we also have the following by the definition of absolute value

$$|a| = (-a), |b| = (-b)$$

By substitution we have

$$|ab| = (-a) \cdot (-b) = |a| \cdot |b|$$

Third case: a is negative, b is positive. Then we have

$$a < 0, b > 0$$

By the additive inverse we know

$$a + (-a) = 0$$

by the definition of absolute value

$$|a| = (-a), |b| = b$$

Using Part II of the EPI we have

$$(-a) \cdot b = -(ab)$$

By the closure and definition of absolute value we have

$$|ab| = -(ab)$$

Finally, by substitution we have

$$|ab| = |a||b|$$

Without the loss of generality, we can let a be positive and b be negative but the procedure is exactly the same was the third case with a and b variable switched. Hence, we have finished the proof.

Zhewen Zheng
University of Washington

Problem 1:

The following proposition is true, but its proof is incorrect. Identify any errorsin the proof. Then provide a correct, well-written and structured proof.

Proposition *Let $n \in \mathbb{Z}$ If n^k is odd for some $k \in \mathbb{N}$, then n is odd.*

Proof. We will prove this proposition by contrapositive. Let n be an integer that is not odd. By 2. on page 10, we know that every integer is either even or odd (and not both). This means that n must be even. Therefore $n = 2m$ for some integer m. Thus for $k = 1, m^k = n^1 = 2m$, which is even and thus not odd. Thus there is some $k \in \mathbb{Z}$ such that n^k is not odd. ∎

Solution:

The contrapositive in the proof above is incorrect. The proof should prove n^k is even for all cases of k rather than the existence of one k. The contrapositive of the proposition should be:

Proposition *Let $n \in \mathbb{Z}$. If n is even, then for all $k \in \mathbb{N}$ it holds that n^k is even .*

Proof. we will prove this proposition by contrapositive. By definition of even, we know that

$$n = 2m$$

for some integer m. For a arbitrary $k \in \mathbb{N}$, by substitution,

$$\begin{aligned} n^k &= (2m)^k \\ n^k &= \underbrace{(2m) \cdot (2m) \cdots (2m)}_{k} \end{aligned}$$

Thus, we have

$$\begin{aligned} n^k &= 2^k(m^k) \\ n^k &= 2(2^{k-1})(m^k) \\ n^k &= 2((2^{k-1})(m^k)) \end{aligned}$$

By closure, $((2^{k-1})(m^k))$ is an integer. Then, by definition of even, for all $k \in \mathbb{N}$ it holds that n^k is even. ∎

Zhewen Zheng
University of Washington

Problem 1:

Let A, B be sets. Prove the following.

(a) $A \subseteq B$ if and only if $A \cup B = B$.

(b) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

(c) In (b), show that $\supseteq$ does not hold in general.

(d) Evaluation of Proofs. What do you think about the following proof. Tell me, what is wrong about the proof. Give a better one if statement is correct, otherwise proof that it is false. Let A, B, C be sets. If $A \cap B = A \cup C$ then $B = C$.

Solution:

(a) *Proof.* We will prove both $\Rightarrow$ and $\Leftarrow$ directions.
If any of the occurring sets are empty, the statement is clear.

$\Rightarrow$ Let $a \in A \cup B$.
Then $a \in A$ or $a \in B$.
If $a \in A$ then by hypothesis $a \in B$. If $a \in B$ then it is clear.

$\Leftarrow$ Let $a \in A$.
Then $a \in A$ or $a \in B$.
Then $a \in A \cup B$.
Then by hypothesis $a \in B$. ∎

(b) *Proof.* We will prove this theorem by cases. Let $X \in \mathcal{P}(A)$.
The statement means $X \in \mathcal{P}(A)$ or $X \in \mathcal{P}(B)$ then $X \in \mathcal{P}(A \cup B)$.
By definition of $\mathcal{P}(A)$ we know that $X \subseteq A$.
We want to show that then $X \subset A \cup B$.
If $X = \emptyset$, this is clear.
If $x \in X$ then $x \in A$, thus $x \in A$ or $x \in B$, this $x \in A \cup B$.
This means $X \subseteq A \cup B$, which means $X \in \mathcal{P}(A \cup B)$. Without the loss of generality, suppose $X \in \mathcal{P}(B)$, we can prove in the same manner that $X \in \mathcal{P}(A \cup B)$. ∎

(c) *Proof.* The statement $\mathcal{P}(A) \cup \mathcal{P}(B) \supseteq \mathcal{P}(A \cup B)$ is understood as the following.
If $X \in \mathcal{P}(A \cup B)$ then $X \in \mathcal{P}(A)$ or $X \in \mathcal{P}(B)$. This is false. Suppose $A = \{1, 2\}, B = \{2, 3\}$.
Then we have

$$\begin{aligned} A \cup B &= \{1, 2, 3\}, \\ \mathcal{P}(A) &= \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}, \\ \mathcal{P}(B) &= \{\emptyset, \{2\}, \{3\}, \{2, 3\}\} \end{aligned}$$

Hence,

$$\mathcal{P}(A) \cup \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{1,2\}, \{2,3\}\},$$
$$\mathcal{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

Clearly there are $X \in \mathcal{P}(A \cup B)$ where $X \notin \mathcal{P}(A)$ and $X \notin \mathcal{P}(B)$, such as $X = \{1,2,3\}$. ■

(d) This proof is incorrect, and the statement is false too. A counterexample to the proof is $A = \emptyset$. B and C can be arbitrary set, while $A \cap B = A \cap C = \emptyset$, B and C does not have to be equal.

Zhewen Zheng
University of Washington

Prove the following two statements by induction.

(a) For all $n \in \mathbb{N}$: $8 \mid 3^{2n} - 1$.

(b) For all $n \in \mathbb{N}$: $\sum_{k=1}^{2n} \frac{(-1)^{k+1}}{k} = \sum_{k=n+1}^{2n} \frac{1}{k}$.

Solution:

(a) *Proof.* Proof: By Induction

Base Case: Let $n = 1$. Then $3^{2 \cdot 1} - 1 = 8$ and $8 \mid 8$.
IH: Assume $8 \mid 3^{2k} - 1$.
Induction Step:

We know that $8 \cdot l = 3^{2k} - 1$ for some $l \in \mathbb{N}$.
Then

$$\begin{aligned} 3^{2(k+1)} - 1 &= 3^{2k+2} - 1 \\ &= 3^2 \cdot 3^{2k} - 1 \\ &= 9(8l + 1) - 1 \\ &= 72l + 9 - 1 \\ &= 72l + 8 \\ &= 8(9l + 1) \end{aligned}$$

Proving that $8 \mid 3^{2(k+1)} - 1$
By the PMI the statement is therefore true. ∎

(b) *Proof.* Proof: By Induction

Base Case: Let $n = 1$. Then $\sum_{k=1}^{2n} \frac{(-1)^{k+1}}{k} = 1 + -\frac{1}{2} = \frac{1}{2} \sum_{k=n+1}^{2n} \frac{1}{k}$.
IH: Assume $\sum_{k=1}^{2l} \frac{(-1)^{k+1}}{k} = \sum_{k=l+1}^{2l} \frac{1}{k}$.
Induction Step:

Then

$$\begin{aligned}
\sum_{k=1}^{2(l+1)} \frac{(-1)^{k+1}}{k} &= \sum_{k=1}^{2l} \frac{(-1)^{k+1}}{k} + \frac{(-1)^{2l+2}}{2l+1} + \frac{(-1)^{2l+3}}{2l+2} \\
&= \sum_{k=l+1}^{2l} \frac{(-1)^{k+1}}{k} + \frac{1}{2l+1} - \frac{1}{2l+2} \\
&= \left(\sum_{k=l+2}^{2l+2} \frac{1}{k} + \frac{1}{l+1} - \frac{1}{2l+1} - \frac{1}{2l+2} \right) + \frac{1}{2l+1} - \frac{1}{2l+2} \\
&= \sum_{k=l+2}^{2l+2} \frac{1}{k} + \frac{1}{l+1} - \frac{1}{2l+1} - \frac{1}{2l+2} + \frac{1}{2l+1} - \frac{1}{2l+2} \\
&= \sum_{k=l+2}^{2l+2} \frac{1}{k} + \frac{1}{l+1} - \frac{2}{2l+2} \\
&= \sum_{k=l+2}^{2l+2} \frac{1}{k} + \frac{1}{l+1} - \frac{1}{l+1} \\
&= \sum_{k=l+2}^{2l+2} \frac{1}{k} \\
&= \sum_{k=(l+1)+1}^{2(l+1)} \frac{1}{k}
\end{aligned}$$

Proving that $\sum_{k=1}^{2(l+1)} \frac{(-1)^{k+1}}{k} = \sum_{k=(l+1)+1}^{2(l+1)} \frac{1}{k}$.
By the PMI the statement is therefore true. ∎

Zhewen Zheng
University of Washington

Katie koscho & Zhewen Zheng & Jordan Hollier

Problem 1:

Equivalence classes really separate elements in A in a very strict way. No two equivalence classes intersect, altogether they give A back. Working with the definition of equivalence class (R,S,T) and the definition of equivalence class prove the mentioned properties.

(a) If $a, b \in A$, then $a \nsim b$ if and only if $[a]_R \cap [b]_R = \emptyset$.

(b) If $a, b \in A$, then if $[a]_R \cap [b]_R \neq \emptyset$ the $[a]_R = [b]_R$

(c) For all $a \in A$, $[a]_R \neq \emptyset$.

Solution:

(a) *Proof.* We will prove both $\Rightarrow$ and $\Leftarrow$ directions.

$\Rightarrow$ We will use proof by contrapositive. Suppose $[a]_R \cup [b]_R \neq \emptyset$. Let $x \in [a]_R \cap [b]_R$. Then

$$a \sim x \text{ and } b \sim x$$

By symmetry we have

$$a \sim x \text{ and } x \sim b$$

and by transitivity we conclude $a \sim b$.

$\Leftarrow$ We will use proof by contrapositive. Suppose $a \sim b$. Then

$$b \in [a]$$

By reflexivity we have

$$b \in [b]$$

Therefore $b \in [a] \cap [b]$ and $[a] \cap [b] \neq \emptyset$. ∎

(b) *Proof.* We will prove both $\subseteq$ and $\supseteq$ directions.

$\subseteq$ Let $x \in [a]_R$. Then

$$a \sim x$$

By hypothesis, there is $y \in A$ such that $a \sim y$ and $b \sim y$.
By symmetry,

$$a \sim y \text{ and } y \sim b$$

By transitivity, $a \sim b$.
By symmetry we also have

$$x \sim a$$

Thus by transitivity we have $x \sim b$, which by symmetry gives $b \sim x$.
Therefore $x \in [b]_R$.

$\supseteq$ Let $x \in [b]_R$. Then

$$b \sim x$$

By hypothesis, there is $y \in A$ such that $a \sim y$ and $b \sim y$.
By symmetry,

$$a \sim y \text{ and } y \sim b$$

By transitivity, $a \sim b$.
By transitivity we have $a \sim x$.
Therefore $x \in [a]_R$. ■

(c) *Proof.* Let a be an element of A. By reflexively, $a \in [a]$. Thus $[a] \neq \emptyset$. ■

Problem 2:

Let R be the relation on the integers defined by $x \sim y$ if and only if $4 \mid (x + 3y)$. Prove that R is an equivalence relation and find its equivalence classes.

Solution:

Proof. Let R be a relation onto A and let x, y and z be elements A. We will prove that R is reflexive, Symmetric, and Transitive.

R Consider $z + 3z = 4z$, there exists an integer z such that $4z = z + 3z$.

S By definition of divisibility, there exists an m such that

$$\begin{aligned} 4m &= x + 3y \\ x &= 4m - 3y \end{aligned}$$

Thus

$$\begin{aligned} y + 3x &= y + 3(4m - 3y) \\ &= 12m - 8y \\ &= 4(3m - 2y) \end{aligned}$$

Let $x \sim y$. By definition of R and definition of divisibility, we have

$$4 \mid y + 3x$$

Thus $y \sim x$.

T Let $x \sim y$ and $y \sim z$, then by definition of R

$$\begin{aligned} 4m &= x + 3y \\ x &= 4m - 3y \\ 4n &= y + 3z \\ 3z &= 4n - y \end{aligned}$$

Consider $x + 3z$, then by the above

$$\begin{aligned} x + 3z &= 4m - 3y + 4n - y \\ &= 4m + 4n - 4y \\ &= 4(m + n - y) \end{aligned}$$

By closure $m + n - y$ is an integer. Thus there exists some integer $m + n - y$ such that $4(m + n - y) = x + 3z$.

Lemma 1
There exist integers x such that $3x = k \mod 4$, where k is any integer from 0 to 3

Proof. Let x be an integer, we will prove there exist x such that $3x \equiv k \mod 4$ where k is an integer from 0 to 3.

x	$3x$	$3x$ (mod 4))
1	3	3
2	6	2
3	9	1
4	12	0

■

Lemma 2
R has 4 equivalence classes.

Proof. Consider $[x]$, this is the set of all y such that $4m = x + 3y$.
By symmetry $4n = y + 3x$. Rearranging the above shows that $4n - 3x = y$. Letting n vary shows that. Assume $3x \equiv k \pmod 4$.
Consider $y - k = 4n - 3x - k$. By $3x \equiv k \pmod 4$, there exists some integer l such that $3x - k = 4l$. Thus

$$\begin{aligned} y - k &= 4n - 3x - k \\ &= 4n - 4l \end{aligned}$$

thus $y - k$ is divisible by 4 and by definition, $y \equiv k \mod 4$ By Lemma 1, There exist x such that $3x \equiv k \pmod 4$, where k is any integer from 0 to 3.
Therefore there are 4 equivalence classes. ■

Because $n \in \mathbb{Z}$ the equivalence classes can be shown to be the below

$$\begin{aligned} A_1 &= \{4n + 1 : n \in \mathbb{Z}\} \\ A_2 &= \{4n + 2 : n \in \mathbb{Z}\} \\ A_3 &= \{4n + 3 : n \in \mathbb{Z}\} \\ A_4 &= \{4n : n \in \mathbb{Z}\} \end{aligned}$$

■

Zhewen Zheng
University of Washington

Problem 1:

(a) Prove the following. Don't use an indirect method, instead use congruence. Let a, b be integers. Then $3|a^2 + b^2$ if and only if $3|a$ and $3|b$.

(b) There are infinitely many integers that are not the sum of two cubes. (Consider the situation modulo 9)

Solution:

(a) **Proposition** *Let a, b be integers. Then $3 \mid a^2 + b^2$ if and only if $3 \mid a$ and $3 \mid b$.*

Proof. We will use congruence to prove this.

$\Leftarrow$ $3 \mid a$ and $3 \mid b$ gives us $a \equiv 0 \pmod 3, b \equiv 0 \pmod 3$.
We know that

$$\text{If } a \equiv c \pmod m, b \equiv c \pmod m \text{ then } a + b \equiv c + d \pmod m.$$
$$\text{If } a \equiv c \pmod m, b \equiv c \pmod m \text{ then } a \cdot b \equiv c \cdot d \pmod m.$$

Then $a \cdot a \equiv 0 \cdot 0 \pmod 3, b \cdot b \equiv 0 \cdot 0 \pmod 3)$.
Then $a^2 \equiv 0 \pmod 3), b^2 \equiv 0 \pmod 3$.
Then $a^2 + b^2 \equiv 0 \pmod 3$.

$\Rightarrow$ If $3 \mid a^2 + b^2$ then $a^2 + b^2 \equiv 0 \pmod 3$.

$[a]$	0	1	2	(mod 3)
$[a^2]$	0	1	1	

Same table for b.

$[a^2 + b^2]$	0	1	2	(a^2)
0	0	1	2	
1	1	2	0	
2	2	0	1	
(b^2)				

We see in the table that $a^2+b^2 \equiv 0 \pmod 3$ if and only if $a \equiv \pmod 3$ and $b \equiv 0 \pmod 3$.
Thus If $3 \mid a^2 + b^2$ then $3 \mid a$ and $3 \mid b$.

(b) *Proof.* Let a, b be integers. Then modulo 9.

a	0	1	2	3	4	5	6	7	8	(mod 9)
a^3	0	1	8	0	1	8	0	1	8	

Same table for b.

a^3+b^3	0	1	8	(a^3)
0	0	1	8	
1	1	2	0	
8	8	0	7	
(b^3)				

c	0	1	2	3	4	5	6	7	8	(mod 9)

This table shows that clearly there exists c's that can never be equal to a^3+b^3 no matter which equivalence class a, b had. ∎

Zhewen Zheng
University of Washington

Problem 1:

Let A be a set and $\mathcal{F}$ be a family. If $\bigcup \mathcal{F} \subseteq A$ then $\mathcal{F} \subseteq \mathcal{P}(A)$.

Solution:

Proof. If $\mathcal{F} = \emptyset$ then the statement is clear.
Let X be an arbitrary set such that $X \in \mathcal{F}$.
If $X = \emptyset$, $X \in \mathcal{P}(A)$ and the statement is clear.
Let x be an arbitrary element such that $x \in X$ where $X \neq \emptyset$.
Then by definition of Family Union $x \in \bigcup \mathcal{F}$.
Then by hypothesis $x \in A$.
Then we have $x \in X$ and $x \in A$.
Then $X \subseteq A$.
By the definition of power set, $X \in \mathcal{P}(A)$ where $X \in \mathcal{F}$. Thus $\mathcal{F} \subseteq \mathcal{P}(A)$. ∎

Problem 2:

Consider the set $A = \{X \in \mathcal{P}(\mathbb{Z}), X = \{k, k+2\}\}$. Show that A is countable infinite.

Solution:

Proof. To show that A is countable infinite we need to a bijection $f : A \to \mathbb{Z}$.
$f : A \to \mathbb{Z}, f(x, y) = x$. Claim: f is bijective.
Consider $g : \mathbb{Z} \to A, g(x) = (x, x+2)$ is the inverse of f.

$$g \circ f(x, y) = g(x) = (x, x+2) = \mathrm{id}_A$$
$$f \circ g(x) = f(x, x+2) = x = \mathrm{id}_{\mathbb{Z}}$$ ∎

Thus we have a bijection $f : A \to \mathbb{Z}$, thus $A \sim \mathbb{Z}$.
Since we have proven $\mathbb{Z}$ is countable infinite, A is countable infinite.

Problem 3:

Prove that there are infinitely many integers that are **not** of the form $n^3 + 2m^2$ for integers m, n. (Hint: Consider the situation modulo 8).

Solution:

We want to show that there are integers that cannot be represented by $n^3 + 2m^2$. Let m, n be integers.

Then modulo 8.

n	0	1	2	3	4	5	6	7	(mod 8)
n^3	0	1	0	3	0	5	0	7	

m	0	1	2	3	4	5	6	7	(mod 8)
m^2	0	1	4	1	0	1	4	1	
$2m^2$	0	2	0	2	0	2	2	2	

$n^3 + 2m^2$	0	2	0	2	0	2	0	2	(mod 8)
0	0	2	0	2	0	2	0	2	
1	1	3	1	3	1	3	1	3	
0	0	2	0	2	0	2	0	2	
3	3	5	3	5	3	5	3	5	
0	0	2	0	2	0	2	0	2	
5	5	7	5	7	5	7	5	7	
0	0	2	0	2	0	2	0	2	
7	7	1	7	1	7	1	7	1	

As we can see, this table shows that $n^3 + 2m^2$ never covers all $[0], \cdots, [9]$ equivalence classes. Thus, there are infinitely many integers that are **not** of the form $n^3 + 2m^2$ for integers m, n.

Problem 4:

Let $A, B \subseteq \mathbb{R}$. A function $f : A \to B$ is called **strictly monotonically increasing**, if for all $a, b \in \mathbb{R}$ with $a < b$ it holds that $f(a) < f(b)$. It is called **strictly monotonically decreasing** if for all $a, b \in \mathbb{R}$ with $a < b$, it holds that $f(a) > f(b)$.

(a) Show that a strictly monotonically increasing function is injective.

(b) Is a monotonically increasing function always surjective? Justify.

(c) Let $f : A \to B$ be strictly monotonically decreasing and $g : B \to C$ be strictly monotonically increasing. Show that $g \circ f$ is strictly monotonically decreasing.

(d) Prove that if $f : A \to B$ is strictly increasing and surjective then the inverse function f^{-1} is also strictly monotonically increasing.

Solution:

(a) **Proposition** *A strictly monotonically increasing function is injective.*

Proof. Let $x_1, x_2 \in A$ with $x_1 < x_2$.
Since f is strictly monotonically increasing, $f(x_1) < f(x_2)$, and in particular $f(x_1) \neq f(x_2)$ for all distinct x_1, x_2 where $x_1 \neq x_2$.
Thus we know that f is injective. ∎

(b) **Proposition** *A monotonically increasing function always surjective.*

Proof. No. This is false. Let's find a counterexample.
Let $A = \mathbb{Z}, \subseteq \mathbb{R}, B = \mathbb{Z} \subseteq \mathbb{R}$.
Consider $f : A \to B, f(x) = 2x$.
Consider $1 \in \mathbb{Z}$.

$$\begin{aligned} f(x) &= 1 \\ 2x &= 1 \\ x &= \frac{1}{2} \\ x &\notin \mathbb{Z} \end{aligned}$$

Therefore f is not surjective. ∎

(c) *Proof.* Let $x_1, x_2 \in A, x_1 < x_2$.
Then since f is strictly monotonically decreasing,

$$f(x_1) > f(x_2)$$

Let $y_1 = f(x_1), y_2 = f(x_2)$. $y_1, y_2 \in B$.
Then, since g is strictly monotonically increasing and $y_1 > y_2$

$$\begin{aligned} g(y_1) &> g(y_2) \\ g(f(x_1)) &> g(f(x_2)) \end{aligned}$$

Thus, for all $x_1 < x_2$

$$g \circ f(x_1) > g \circ f(x_2)$$

Therefore $g \circ f$ is strictly monotonically decreasing. ∎

(d) **Proposition** *If $f : A \to B$ is strictly increasing and surjective then the inverse function f^{-1} is also strictly monotonically increasing.*

Proof. Let $f : A \to B$ be strictly increasing and surjective.
We have proven $f : A \to B$ is injective. Thus f is bijective.
Then there is a well-defined inverse f^{-1}.
Now we use proof by contradiction. Let $y_1, y_2 \in B, y_1 < y_2$.
We are trying to prove that

$$f^{-1}(y_1) < f^{-1}(y_2)$$

Assume

$$f^{-1}(y_1) \geq f^{-1}(y_2)$$

We know that $y_1 \neq y_2$, and because f^{-1} is bijective, $f^{-1}(y_1) \neq f^{-1}(y_2)$.
Thus $f^{-1}(y_1) > f^{-1}(y_2)$.
Then

$$\begin{aligned} f \circ f^{-1}(y_1) &> f \circ f^{-1}(y_2) \\ y_1 &> y_2 \end{aligned}$$

This is a contradiction to $y_1 < y_2$. Therefore,

$$f^{-1}(y_1) < f^{-1}(y_2)$$

and f^{-1} is strictly monotonically increasing. ■

Problem 5:

Fermat's little theorem. Little Fermat. Let a be an integer and let p be a prime. Then

$$a^p \equiv a \pmod{p}.$$

You can use the binomial formula without proof: $(x+y)^k = \sum_{j=0}^{k} \binom{k}{j} x^j y^{k-j}$. Use induction and clearly mark where the fact is used that p is a prime (for this consider what happens when we don't have a prime, see the 'counter'-example 6 and $\binom{6}{2}$).

Solution:

Proposition *Let a be an integer and let p be a prime. Then*

$$a^p \equiv a \pmod{p}.$$

Proof. We will prove the negative part and the nonnegative part of a separately.
For the nonnegative part, we will use proof by induction.
Let a be an nonnegative integer and p be a prime.

- Base Case: $0^p \equiv 0 \pmod{p}$
- Inductive Hypothesis: $a^p \equiv a \pmod{p}$.
- Inductive Step: We will show $(a+1)^p \equiv a+1 \pmod{p}$.
  By the binomial theorem,

$$\begin{aligned}
(a+1)^p &= \sum_{j=0}^{p} \binom{p}{j} a^j 1^{p-j} \\
&= \sum_{j=0}^{p} \binom{p}{j} a^j \\
&= \sum_{j=0}^{p} \frac{p!}{j!(p-j)!} a^j \\
&= 1 + \frac{p!}{1!(p-1)!} a^1 + \frac{p!}{2!(p-2)!} a^2 + \cdots + \cdots + \frac{p!}{(p-1)!1!} a^{p-1} + a^p \\
&= 1 + \sum_{j=1}^{p-1} \left(\frac{p!}{j!(p-j)!} a^j \right) + a^p
\end{aligned}$$

To take the modulo p on the binomial expansion of $(a+1)^p$ we can take the modulus on each individual terms and sum it up.
For 1, $1 \equiv 1 \pmod{p}$.
For a^p, $a^p \equiv a \pmod{p}$ by the Induction Hypothesis

For $\sum_{j=1}^{p-1}\left(\frac{p!}{j!(p-j)!}a^j\right)$, notice that since p is a prime, the numerator of $\frac{p!}{j!(p-j)!}$ always has a non-factorizable factor of p. This means that p always divides each terms of this summation. Hence, $\sum_{j=1}^{p-1}\left(\frac{p!}{j!(p-j)!}a^j\right) \equiv 0 \pmod{p}$. Therefore, adding up the terms, we have

$$1+\sum_{j=1}^{p-1}\left(\frac{p!}{j!(p-j)!}a^j\right)+a^p \equiv 1+0+a \pmod{p}$$
$$1+\sum_{j=1}^{p-1}\left(\frac{p!}{j!(p-j)!}a^j\right)+a^p \equiv a+1 \pmod{p}$$
$$(a+1)^p \equiv a+1 \pmod{p}$$

By the PMI, we conclude that $a^p \equiv a \pmod{p}$ for nonnegative-integer a and prime number p.

Now, let's prove $(-a)^p \equiv (-a) \pmod{p}$ for prime numbers $p \neq 2$. Since we have proven $a^p \equiv a \pmod{p}$ for nonnegitive integer a and prime p, we have

$$a^p \equiv a \pmod{p}$$
$$(-1)a^p \equiv (-1)a \pmod{p}$$

For prime $p \neq 2$,

$$(-1)^p = (-1)$$

Thus we have

$$(-1)^p a^p \equiv (-1)a \pmod{p}$$
$$(-a)^p \equiv (-a) \pmod{p}$$

For prime number $p \neq 2$. For prime number $p = 2$,

$$b^2 = (-a)^2 = a^2$$

and a is a nonnegative integer. Thus we can use our previous conclusion for nonnegative integer a. We know that

$$a^2 \equiv a \pmod{2}$$

Notice that

$$2a \equiv 0 \pmod{2}$$
$$a \equiv -a \pmod{2}$$

and since equivalence is transitive

$$a^2 \equiv -a \pmod{2}$$

By substitution

$$(-a)^2 \equiv -a \pmod 2$$

Therefore, we have proven that for all integers a and all prime p,

$$a^p \equiv a \pmod p$$ ■